ارتباط امن
Ertebate Amn

به ارتباط امن بپیوند

معرفی محصول
Venustech IFW

IFW-3000 V5.0

فهرست مطالب

- مشخصات سخت افزاری
- عملکردهای نرم افزاری
  - وضعیت سیستم
  - مدیریت سیستم
  - کشف شبکه
  - تنظیم سرویس ها (Service rules)
  - تنظیم سیاست ها (Policy rules)
  - VPN صنعتی
  - Serial DPI
  - High availability
  - Log
- کاربردهای معمول

مشخصات سخت افزاری

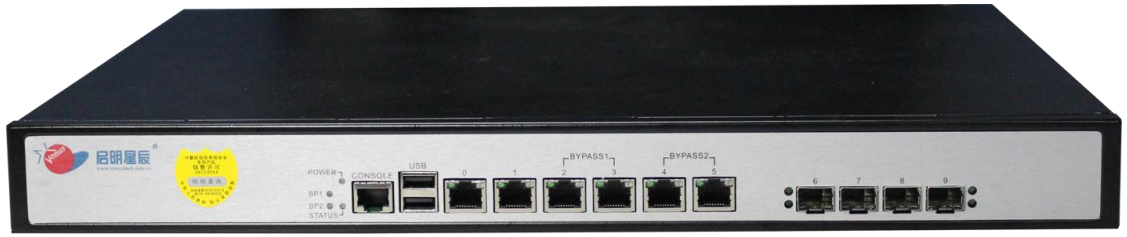
مشخصات
سخت افزاری

سری Venusense IFW-3000

2-port guide rail mounted

5-port guide rail mounted

6-port rack mounted



6-electrical +4-optical rack mounted

قابل استفاده درانواع شبکه های صنعتی

سازگار با محیط های صنعتی با شرایط سخت

مصرف برق بسیار کم

تحمل دامنه وسیع تغییر دما
:Storage
-40~85 °C
دمای کاری:
-40~75 °C

دارای افزونگی در منبع برق (9-48 V DC)

مناسب بکارگیری در محیط تولیدی صنعتی
جهت محافظت از PLC و ایستگاه کاری مهندس سیستم

اولین فایروال در صنعت که با استانداردهای ارتباط سریال (RS232 & RS485) سازگار است

Plug-and-play

نصب بر روی ریل

دارای امکان Bypass

طراحی بدون فن

طراحی صنعتی، پایدار و قابل اطمینان

سازگار با محیط های صنعتی با شرایط سخت

مناسب بکارگیری در اتاق تجهیزات محیط های صنعتی
جهت محافظت از انتقال داده صنعتی

Rack mounted

دامنه تحمل دمای محیط کاری:
-5~45 °C

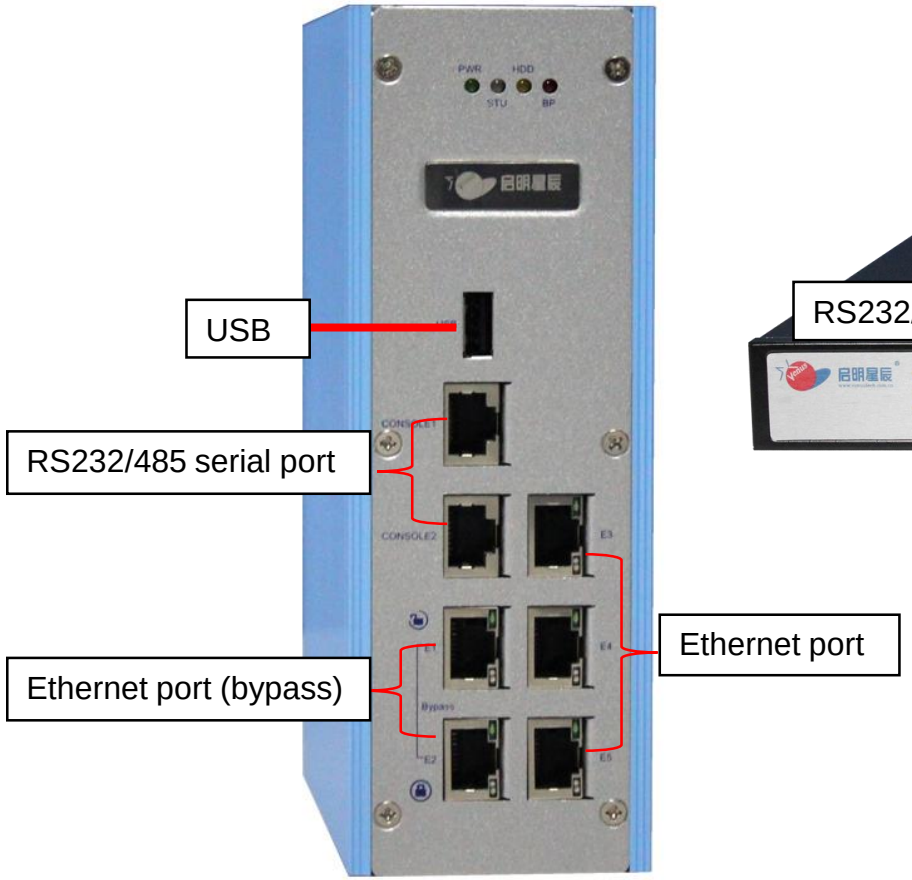
دارای امکان Bypass

6*GE ports

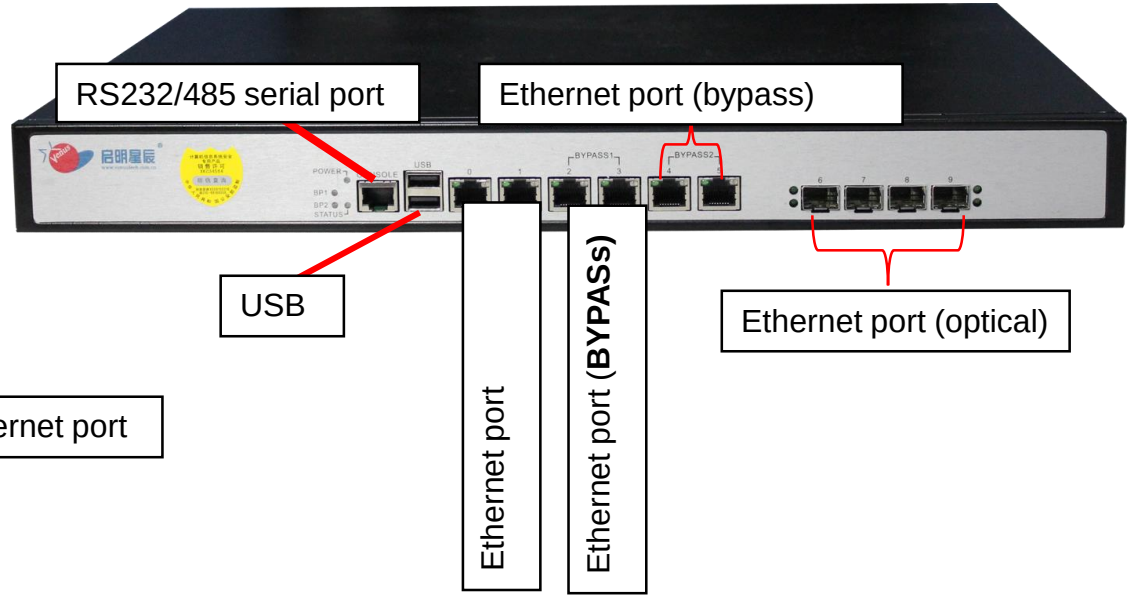
طراحی بدون فن

Portها در فایروال صنعتی سری ۳۰۰۰

Guide rail mounted



Rack mounted



مشخصات محصولات

Item	201D	302D	1100R	1100R-R	1100R-GR
Type	**DIN guide rail**	**DIN guide rail**	**Rack**	**Rack**	**Rack**
Network port	2*GE electrical	5*GE electrical	6*GE electrical	6*GE electrical	6*GE electrical + 4*GE optical
Serial port	2*serial, supporting RS232/485	2*serial, supporting RS232/485	1*serial	1*serial	1*serial
Fanless	√	√	√	√	√
Bypass	√	√	√	√	√
Power redundancy	Dual-power redundancy	Dual-power redundancy	Single power	Dual-power redundancy	Dual-power redundancy
Working temperature	-40-70°C	-40-70°C	-5-40°C	-5-40°C	-5-40°C
Concurrent connections	480,000	480,000	500,000	500,000	500,000
New connections per second	6,500	6,500	9,000	9,000	9,000
Throughput	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps

عملکردهای نرم افزاری

۱. وضعیت سیستم

پایش وضعیت

- وضعیت فایروال
  - ✓ پایش و مشاهده میزان استفاده از CPU و Memory
  - ✓ نسخه سخت افزار و نرم افزار و سایر اطلاعات مربوطه
  - ✓ تعداد و وضعیت Port ها
- سرویس ها و سیاست ها (Policies & Services)
  - ✓ تعداد دارایی های محافظت شده
  - ✓ تعداد Rule های تنظیم شده
  - ✓ ترافیک شبکه، تعداد Session ها و ۱۰ تا IP برتر
  - ✓ توزیع پروتکل سرویس ها
- اجازه ها و رخدادها (Authorization & Log)
  - ✓ اطلاعات مجوزهای هر ماژول
  - ✓ اطلاعات رخدادها

۱ – وضعیت سیستم – وضعیت فایروال

وضعیت فایروال

Device information

Current mode : All passing mode Setting mode

وضعیت سیستم

System information

Software name : themis

Software version : 5.0.0.1(2236)

Hardware version : 天清汉马工业防火墙系统V5.0(IFW-3000-302D)

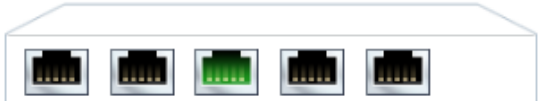
Serial number : 701eef4bc946e67c

Industrial VPN service : Already stopped

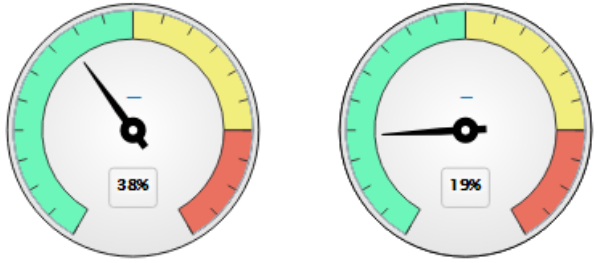
Device HA service : Active/Standby Close

Interface information

Interface	IP address	Transmit	Receive
eth0		0bps	0bps
eth1		0bps	0bps
eth2	172.16.2.245	26712bps	15608bps
eth3		0bps	0bps
eth4		0bps	0bps



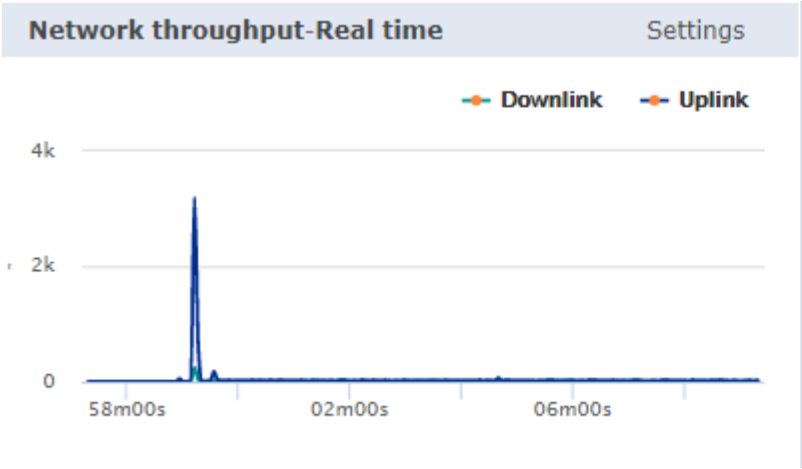
اطلاعات Port ها

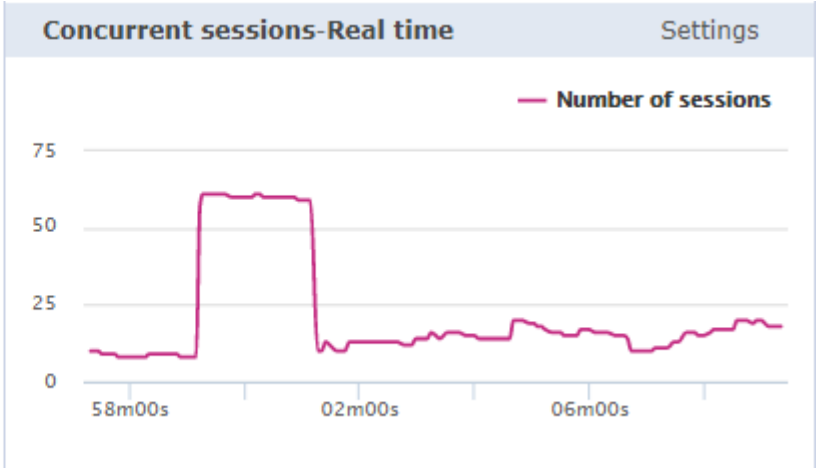


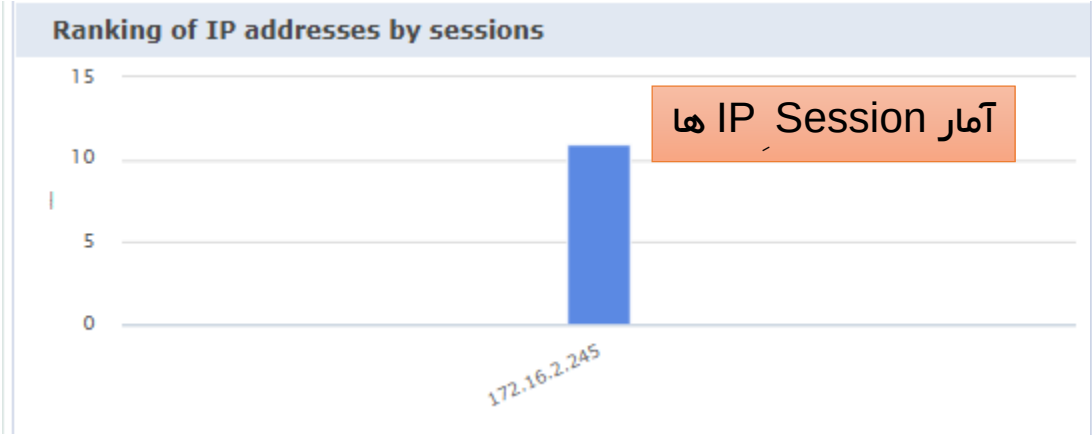
پردازشگر و حافظه

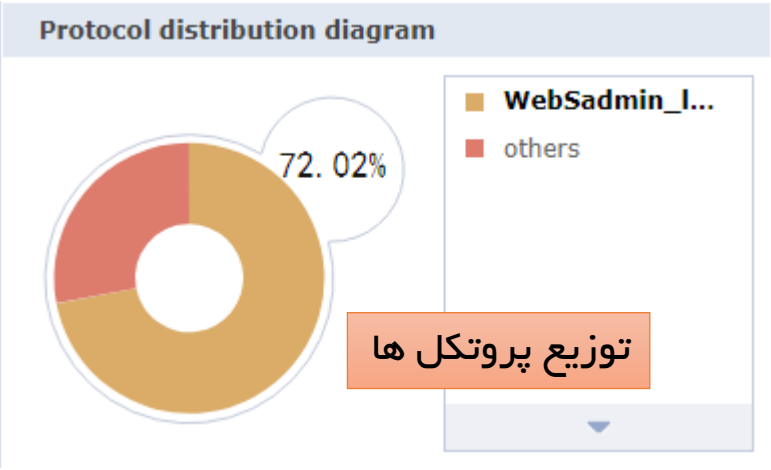
۱ – وضعیت سیستم – سیاست ها و حجم سرویس

آمار ترافیک شبکه



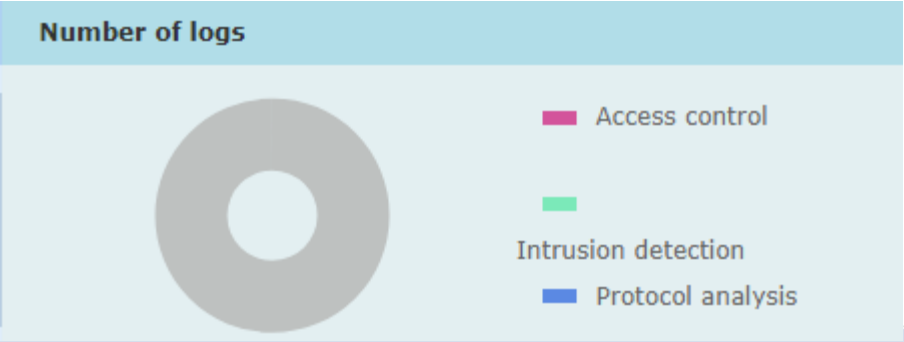






۱ – وضعیت سیستم – اجازه ها و رخدادها

رخدادها



Log information

Date/Time	Type	Level	Details
2017/10/18 09:59:11	Management log	Tips	The administrator [administrator] has logged in successfully from [172.16.2.8].
2017/10/18 09:58:20	Management log	Tips	Administrator [administrator] access timeout.
2017/10/18 09:56:20	Management log	Notice	Administrator [administrator] runs command View session management - session statistics connection statistics.
2017/10/18 09:56:18	Management log	Notice	Administrator [administrator] runs command View session management - session statistics connection ranking.
2017/10/18 09:56:13	Management log	Notice	Administrator [adı statistics.

اجازه ها

licenseInformation

Module name	Closing time	Description	State
OPC	2018/01/14 17:57:59		Already trialed
EIP	2018/01/14 17:58:04		Already trialed
Modbus	2018/01/14 17:58:10		Already trialed

۱ – وضعیت سیستم – آمار Sessionها

تعداد ارتباطات

Total number of connections	
IPV4	14
TCP	13
UDP	1
ICMP	0
Protocol	0

TCP connection	
NONE	0
SYN_SENT	0
SYN_RECV	0
ESTABLISHED	12
FIN_WAIT	0
CLOSE_WAIT	0
LAST_ACK	0
TIME_WAIT	0

لیست رتبه ارتباطات

Connection statistics | Connection ranking

Set refreshing time: 10Second

Source connection ranking

Ranking	IP	Number of connections
1	172.16.2.8	32
2	127.0.0.1	8

Ranking of destination connections

Ranking	IP	Number of connections
1	172.16.2.245	32
2	127.0.0.1	8

۲- مدیریت سیستم – تنظیمات سیستم (۱)

◻ تاریخ و ساعت

- ➢ هماهنگ سازی زمان سیستم
  - ✓ هماهنگ کردن با کامپیوتر مدیریت کننده فایروال
- ➢ تنظیم منطقه زمانی
  - ✓ تنظیم منطقه زمانی با توجه به ناحیه جغرافیایی
- ➢ استفاده از سرور زمان
  - ✓ با استفاده از آدرس IP
  - ✓ با استفاده از نام در دامین
  - ✓ تنظیم فاصله زمانی هماهنگ سازی با توجه به نیاز

۲- مدیریت سیستم – تنظیمات سیستم (۱)

هماهنگ سازی زمان سیستم

Date and time

Device time:	2017-10-18 10:59:32
Host time:	2017-10-18 10:59:26 Time synchronization

تنظیم منطقه زمانی

Time zone setting

Time zone: (GMT+8) Beijing, Hor ▾ OK

(GMT-12) Eniwetok Atoll, Kwajalein Atoll
(GMT-11) Midway Islands, Samoa Islands

Clock server

تنظیم سرور زمان

Clock server

Enable clock server:	☑
IP settings:	◉ 10.10.10.252 Synchronize now
Domain name settings:	○
Synchronization interval (in minutes):	100
	OK

۲- مدیریت سیستم – تنظیمات سیستم (۲)

پارامترهای سیستم

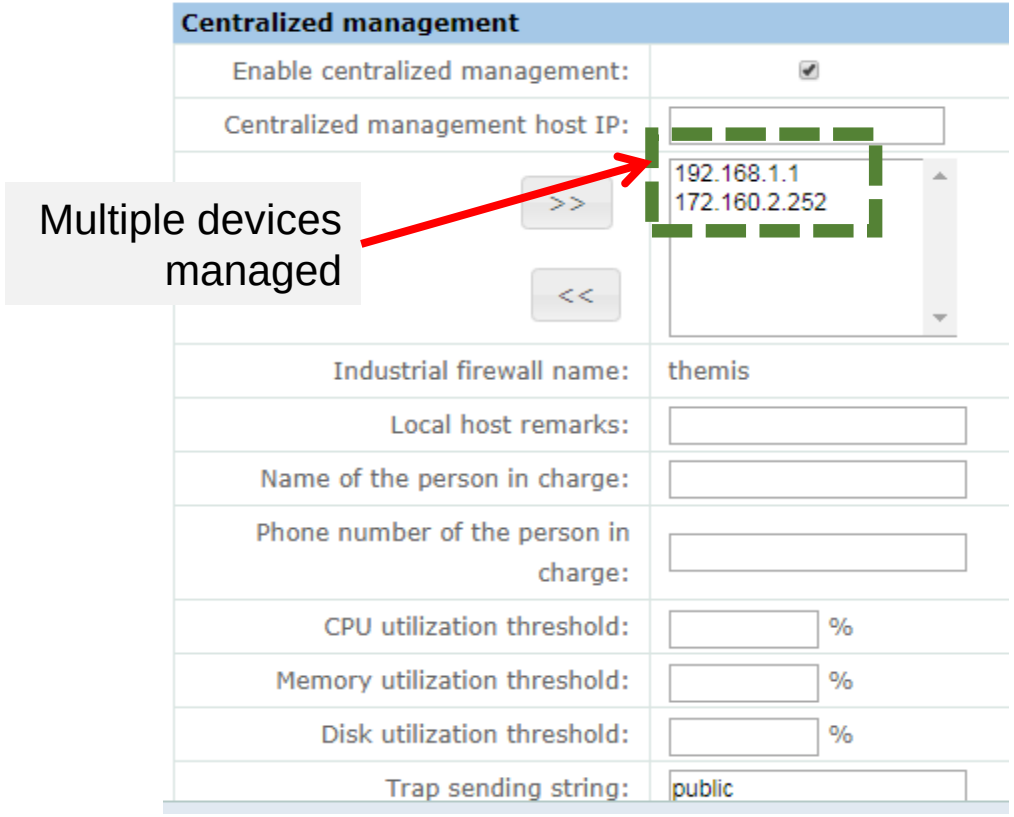
- نام دستگاه
  - ✓ این نام با توجه به سلیقه کاربر و الزامات داده ها در پروژه قابل تغییر است
- شماره سریال
  - ✓ شماره تشخیص منحصر بفرد و غیر قابل تغییر محصول
  - ✓ برای نصب لایسنس و نگهداری سیستم مورد نیاز می باشد*
- تنظیمات پارامترهای سخت افزاری غیر قابل تغییر می باشد

System information

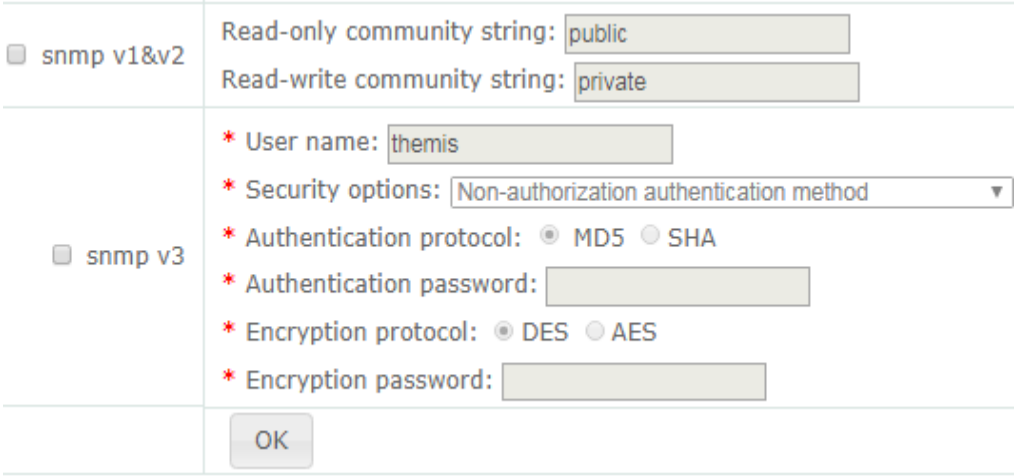
Sequence number	Parameter name	Parameter value	Remarks	Operation
1	Host name	themis	Local host name	Edit
2	Serial number	701eef4bc946e67c	Local host serial number	
3	Hardware configuration	2000000	Local host hardware configuration	

۲– مدیریت سیستم – تنظیمات سیستم (۳)

- مدیریت امنیت
  - رابط استاندارد SNMP
  - پشتیبانی از SNMPv1-v3
  - امکان مدیریت امنیت از طریق چندین دستگاه مشخص
  - امکان مدیریت توسط SOC



SNMPv1-v3



۲- مدیریت سیستم – تنظیمات سیستم (۴)

تنظیمات مدیر سیستم

- تنظیمات دسترسی
  - Super administrator / Security administrator / Audit administrator / System administrator

- اضافه کردن، حذف کردن، تغییر دادن و Query زدن
  - امکان ایجاد حساب های کاربری با دسترسی مختلف بر اساس نیاز
  - امکان حذف حساب های کاربری ایجاد شده توسط مدیر سیستم
  - عدم امکان حذف حساب های کاربری پیش فرض
  - امکان تغییر دسترسی های حساب های کاربری ایجاد شده
  - امکان Query زدن بر روی اطلاعاتی مانند نام کاربر، دسترسی ها و تعداد حساب های کاربری

- مدیریت چند-کاربره
  - چندین کاربر امکان کار کردن همزمان با دستگاه را دارند

- کنترل پیچیدگی رمز عبور و آنتی-کرک
  - پیچیدگی رمز عبور: ۸ تا ۱۵ کاراکتر با در نظر گرفتن کوچک بودن یا بزرگ بودن، شامل اعداد و کاراکترهای خاص
  - عدم امکان ورود به سیستم در صورتیکه تعداد تلاش های ناموفق پشت سرهم جهت ورود از ۵ بیشتر شود

۲- مدیریت سیستم – تنظیمات سیستم (۴)

۲– مدیریت سیستم – تنظیمات سیستم (۵)

- دستگاه مدیریت کننده
  - محدود کردن مدیریت دستگاه به آدرس های مشخص
  - حداکثر ۵ تا آدرس می توان داد
  - آدرس ها: یک دستگاه، یک شبکه، همه
  - امکان استفاده از White list

Management host

Sequence number	Management host IP	Subnet mask	Description	Operation
1	10.1.5.200	255.255.255.255	IPv4管理主机1...	Edit Delete
2	0.0.0.0	0.0.0.0		Edit Delete
3	10.1.4.0	255.255.255.0	TEST	Edit Delete
4	192.168.0.0	255.255.0.0		Edit Delete
5	10.0.0.0	255.0.0.0		Edit Delete

Add Centralized management host

۲- مدیریت سیستم – تنظیمات سیستم (۶)

- مدیریت گواهینامه
  - روش پیش فرض احراز هویت مدیر سیستم:
    - گواهینامه + رمز عبور
  - زنجیره گواهینامه و گواهینامه های تعبیه شده
    - گواهینامه های غیر قابل تغییر
  - احراز هویت گواهینامه دوطرفه بین فایروال و دستگاه مدیر

Administrator certificate

CA certificate:	OCAforSSLVPN
Device certificate:	Default gateway certificate
	OK
Administrator certificate:	Please select
	OK

Administrator certificate list

Effective	Certificate name	Details	Operation
☑	Default administrator certificate	Subject: C=CN, O=Venus, OU=Venus VPN, CN=10.1.5.200 Issuer: C=CN, O=Venus, OU=Venus VPN, CN=OCA Venus VPN Validity period: 2014-6-27 to 2020-9-9	

Show 10 lines | Home | Previous | 1 | Next | Last | Jump to 1 page | GO

Effective

۲- مدیریت سیستم – تنظیمات سیستم (۷)

- نگهداری سیستم

- تهیه نسخه پشتیبان و بازیابی تنظیمات فایروال
  - وارد کردن و خروجی گرفتن فایل های تنظیمات
  - بازیابی تنظیمات پیش فرض کارخانه
  - ذخیره تنظیمات
- بروز رسانی نرم افزار
  - ارتقاء عملکرد
  - ارتقاء شخصی سازی شده
- لایسنس
  - ماژول های موجود در دستگاه و وضعیت ماژول
  - خرید و اضافه کردن لایسنس ماژول
- سیستم دوگانه
  - تهیه نسخه پشتیبان و بازیابی نرم افزار سیستم
  - امکان انتخاب سیستم پیش فرض برای Boot
  - این دو سیستم از یکدیگر مستقل هستند
  - سیستم B بطور پیش فرض خالی می باشد

۲- مدیریت سیستم – تنظیمات سیستم (۷)

Backup and recovery | Upgrade | License | Dual system | Debug

Backup and recovery

Export configuration

Configuration file: Browse... Import configuration

Restore factory settings | Save configuration

تهیه نسخه پشتیبان و بازیابی تنظیمات

Upgrade

Current system software version : 5.0.0.1(2236)

* Upgrade file: Browse... Upgrade

Version upgrade information

ارتقاء عملکرد نرم افزار

Sequence number	after upgrade	Upgrade description	Upgrade time
1	5.0.0.1(2236)	Venus Security Gateway	2017/08/17 10:11:27

Export upgrade records | Reboot device

Import license

Product license Browse... Import

وارد کردن فایل لایسنس

LicenseEnable information

لایسنس ها

Module name	Closing time	Description	State	Operation	Tips
OPC	2018/01/14 17:57:59		Already trialed	Enable	If you need to use it for a long term, please contact the vendor!
EIP	2018/01/14 17:58:04		Already trialed	Enable	If you need to use it for a long term, please contact the vendor!
Modbus	2018/01/14 17:58:10		Already trialed	Enable	If you need to use it for a long term, please contact the vendor!
ModbusRTU	2018/01/14 17:58:16		Already trialed	Enable	If you need to use it for a long term, please contact the vendor!
Industrial VPN	2018/01/14 17:58:26	Number of IPSEC tunnels:50	Already trialed	Enable	If you need to use it for a long term, please contact the vendor!
Industrial IPS	2018/01/14 17:58:32		Already trialed	Enable	If you need to use it for a long term, please contact the vendor!
Industrial IPS signature library	2018/01/14 17:58:38		Already trialed	Enable	If you need to use it for a long term, please contact the vendor!

۲- مدیریت سیستم – تنظیمات سیستم (۷)

سیستم پیش فرض A می باشد و سایر سیستم ها خالی می باشند

System state diagram

systemA	systemB	Backup system
5.0.0.1(2236)		

تنظیم سیستم پیش فرض Boot

Start the system by default

systemA systemB

OK

سیستم پشتیبان – ذخیره تنظیمات فعال بر روی سیستم پشتیبان

Backup system

Back up the current system (systemA[5.0.0.1(2236)]) to the backup system

OK

بازیابی نسخه پشتیبان – بازیابی تنظیمات سیستم پشتیبان بر روی سیستم انتخابی

system recovery

There is no system in the current backup system

systemA systemB

OK

۲– مدیریت سیستم – تنظیمات شبکه (۱)

- رابط Ethernet
  - سرعت کاری
    - ✓ 10/100/1000 Mbps auto-sensing
  - حالت کاری
    - ✓ حالت Routing
      - تنظیم دستی آدرس IP
      - دریافت آدرس IP از DHCP
    - ✓ حالت Transparent
    - ✓ حالت Trunk
  - Line sequence
    - ✓ Crossover/straight-through auto-sensing
  - ویژگی های رابط
    - ✓ امکان فعال کردن Ping
    - ✓ امکان مدیریت کردن
    - ✓ امکان فعال کردن Traceroute
    - ✓ امکان غیرفعال کردن رابط

- رابط سریال
  - RS232, RS485

۲- مدیریت سیستم – تنظیمات شبکه (۱)

Physical device

	Device name	IP address/mask	Operating mode	Obtaining IP address	Whether to enable	Operation
	eth0		Transparent mode	statically specified	✓	Edit
	eth1		Transparent mode	statically specified	✓	Edit
	eth2	172.16.2.245/255.255.255.0	Routing mode	statically specified	✓	Edit
	eth3		Routing mode	statically specified	✗	Edit
	eth4		Routing mode	statically specified	✗	Edit

رابط های فیزیکی

Batch stop | Batch start | Show 10 lines | Home | Previous | 1 | Next | Last | Jump to 1 page | GO

Modify physical device

Interface name: eth0 (Cannot be modified)

Link operating mode: Self-adaption

Operating mode: Transparent mode (Transparent mode / Routing mode / Trunk mode)

Whether to enable:

Advanced options

Remark name: eth0 (1-15 characters, including letters, numbers, minus, and underline)

MAC address: 00:0D:48:26:91:22

MTU: 1500 (68-9216)

Disable ICMP redirect:

تنظیم سرعت رابط

تنظیم حالت کاری رابط

تنظیم گزینه های پیشرفته

۲- مدیریت سیستم – تنظیمات شبکه (۱)

تنظیمات رابط با حالت کاری Routing

Modify physical device

Interface name: eth2 (Cannot be modified)

Link operating mode: Self-adaption

Operating mode: Routing mode

Obtaining IP address: Static IP address

Static IP address
DHCP get

IP address : / 255.255.255.0

For management:

Allow PING:

Allow Traceroute:

Whether to enable:

Advanced options

حالت تنظیم آدرس IP

ویژگی های رابط

Advanced options

Remark name: eth2 (1-15 c
letters, numbers, minus, and underline)

MAC address: 00:0D:48:26:91:19

MTU: 1500 (68-921

Enable dynamic domain:

Dynamic domain name:

Disable ICMP redirect:

Enable anti-ARP attack:

Enable IP address spoofing check:

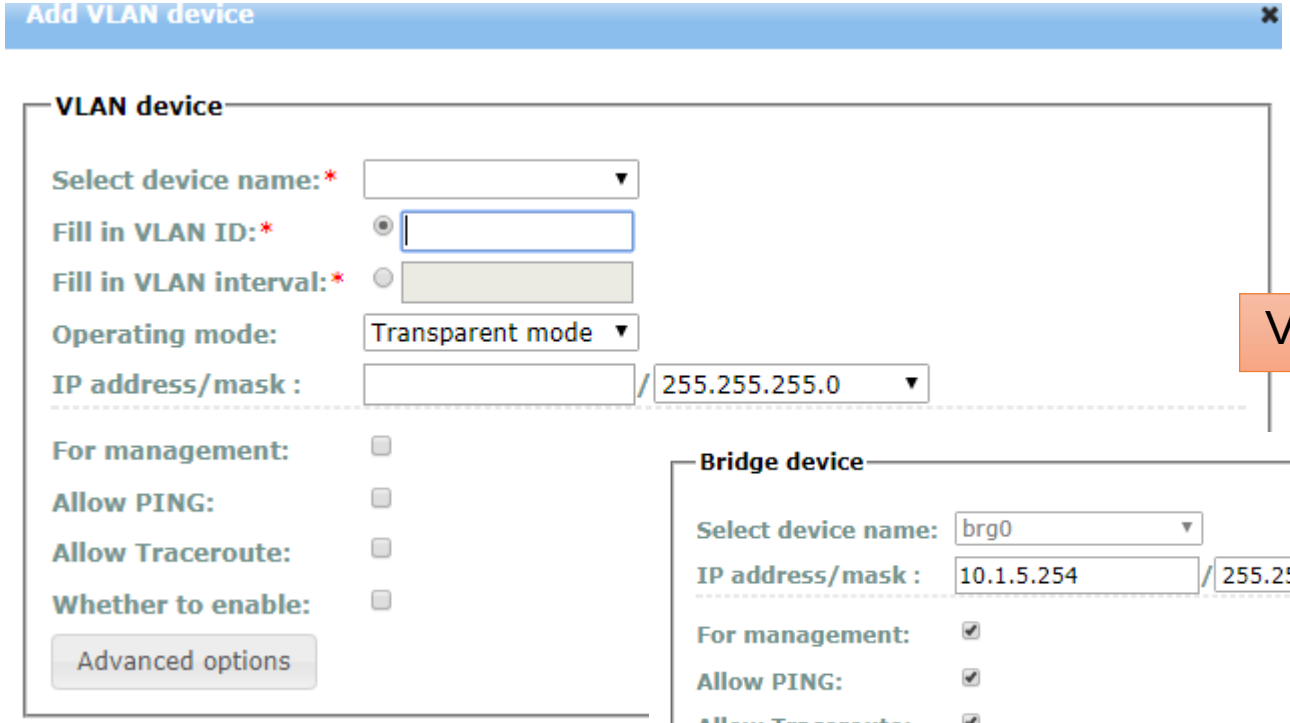
Enable DHCP relay:

DHCP server address: (Multiple IP addresses are separated by commas)

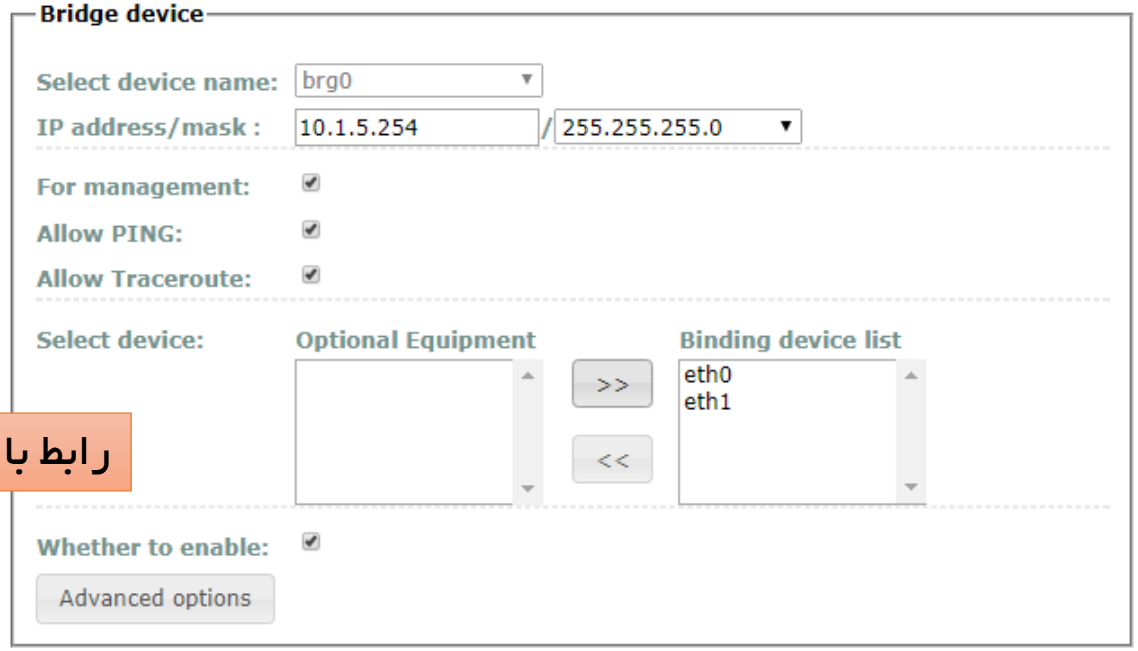
گزینه های پیشرفته رابط

تنظیم سرور DHCP

۲– مدیریت سیستم – تنظیمات شبکه (۱)



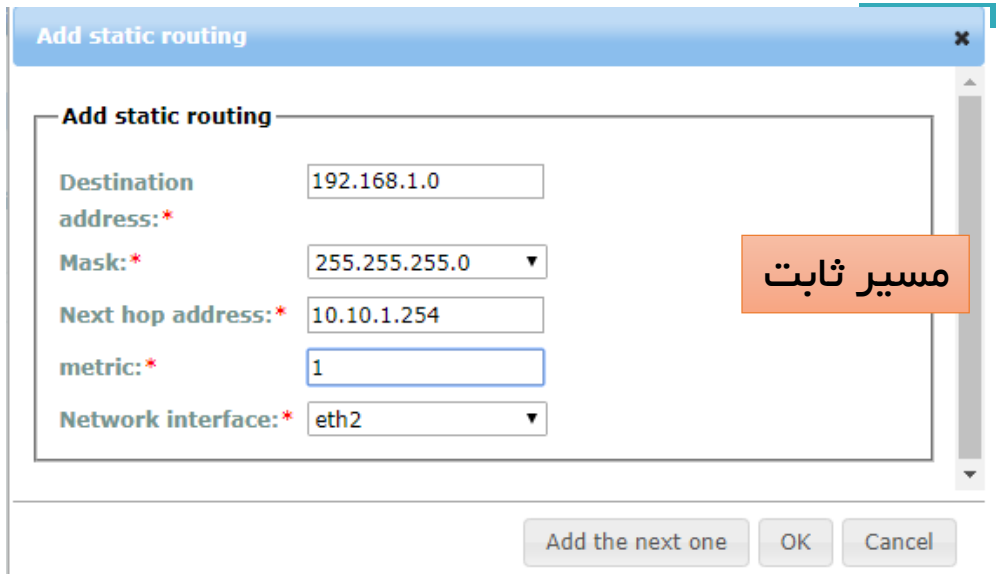
رابط با حالت کاری VLAN/Trunk



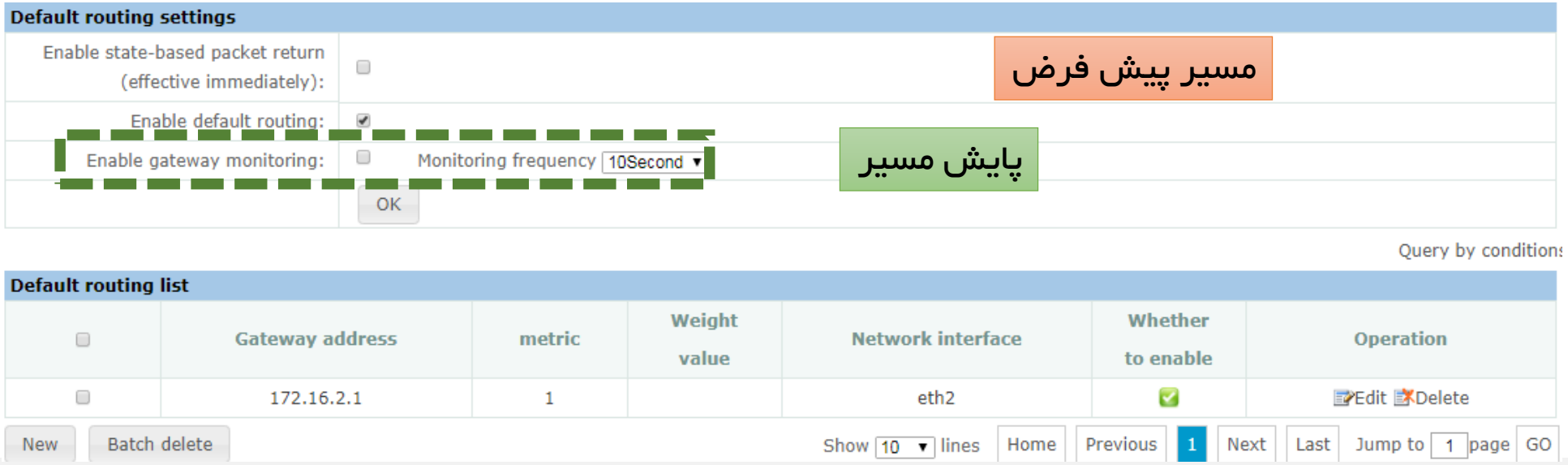
رابط با حالت کاری Transparent

۲- مدیریت سیستم - مسیریابی

- مسیریابی
  - مسیر ثابت
  - مسیر پیش فرض
    - ✓ افزونگی و تقسیم بار با امکان چند-مسیری
    - ✓ پایش مسیر



مسیر ثابت



مسیر پیش فرض

پایش مسیر

۳- کشف شبکه

- یادگیری خودکار از ترافیک

- کشف خوکار تجهیزات داخل شبکه
- یادگیری هوشمند ارتباطات در شبکه
  - ✓ ارتباطات Protocol-based
  - ✓ ارتباطات Flow-based
- کشف مؤثر دستورالعمل های پروتکل های شبکه صنعتی
- نمایش تجهیزات، لایه شبکه و لایه برنامه های کاربردی
- شناخت کامل شبکه و کمک به ایجاد قوانین برای فایروال
- کمک به شناخت پیچیدگی های شبکه
  - ✓ آنالیز و شفاف سازی اجزاء و جریان های داخل شبکه
- امکان ضبط و ذخیره پاکت های شبکه

۳- کشف شبکه

Network discovery

Network discovery :

Enabling network discovery and firewall intelligent learning mode can achieve automatically discover device assets in the network, identify the network connection relationship between device assets and the type of protocol in the network, intelligently analyze industrial protocols and automatically generate protection rules.

Close

غیر فعال شدن اتوماتیک
(۳۰ روز بعد از فعال شدن)

دارایی های تشخیص داده شده پس از فعال کردن

Query by conditions

	Sequence number	Asset name	IP address	MAC address	Vendor name	Operation
	1	QuantaCo1	172.16.2.8	04:7D:7B:14:E1:CB	QuantaCo	Packet capture Edit Delete
	2	RealtekS3	123.151.148.111	00:E0:4C:0B:81:C2	RealtekS	Packet capture Edit Delete
	3	RealtekS4	123.151.77.223	00:E0:4C:0B:81:C2	RealtekS	Packet capture Edit Delete
	4	RealtekS5	125.39.132.163	00:E0:4C:0B:81:C2	RealtekS	Packet capture Edit Delete
	5	RealtekS6	125.39.132.162	00:E0:4C:0B:81:C2	RealtekS	Packet capture Edit Delete
	6	RealtekS7	123.151.77.214	00:E0:4C:0B:81:C2	RealtekS	Packet capture Edit Delete
	7	RealtekS8	183.60.49.182	00:E0:4C:0B:81:C2	RealtekS	Packet capture Edit Delete
	8	RealtekS9	183.60.48.250	00:E0:4C:0B:81:C2	RealtekS	Packet capture Edit Delete
	9	RealtekS10	163.177.94.82	00:E0:4C:0B:81:C2	RealtekS	Packet capture Edit Delete
	10	RealtekS11	183.232.94.217	00:E0:4C:0B:81:C2	RealtekS	Packet capture Edit Delete

Batch delete Clear Show 10 lines Home Previous 1 2 3 Next Last Jump to 1 page GO

نام گذاری: شرکت سازنده، نام، IP، MAC

۳- کشف شبکه

جریان ها

AewinTec22(Asset) — Generate

QuantaCo1(Asset) — Generate

RealtekS10(Asset) — Generate

Object

QuantaCo1	→	RealtekS10	http	Packet capture, Generate policy, Delete
QuantaCo1	→	RealtekS10	https	Packet capture, Generate policy, Delete

پروتکل ها

http(Protocol) — Generate

https(Protocol) — Generate

Object

QuantaCo1	→	RealtekS5	Packet capture, Generate policy, Delete
QuantaCo1	→	RealtekS7	Packet capture, Generate policy, Delete
QuantaCo1	→	RealtekS8	Packet capture, Generate policy, Delete
QuantaCo1	→	RealtekS10	Packet capture, Generate policy, Delete

HIMA_SILworX_ELOP(Protocol) — Generate

ddi-tcp-2(Protocol) — Generate

http-alt(Protocol) — Generate

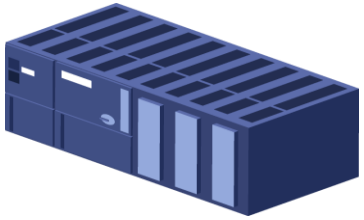
icmp_request(Protocol) — Generate

۴- قوانین امنیتی – پروتکل Modbus

کنترل و محافظت
لایه برنامه کاربردی Modbus

Engineer station

فیلتر کدهای عملکرد (Function Code)	فیلتر جریان اصلی و کدهای عملکرد شخصی سازی شده
کنترل متغیرها	فیلتر ثبات ها، متغیرهای گسسته و شناسه (ID) تجهیزات صنعتی
کنترل صحت	فیلتر پاکت های غیر نرمال و تغییر شکل داده شده
پاسخ به رخدادهای غیر نرمال	پاسخ به رخدادهای غیر نرمال و Reset



PLC
(Programmable Logic Controller)

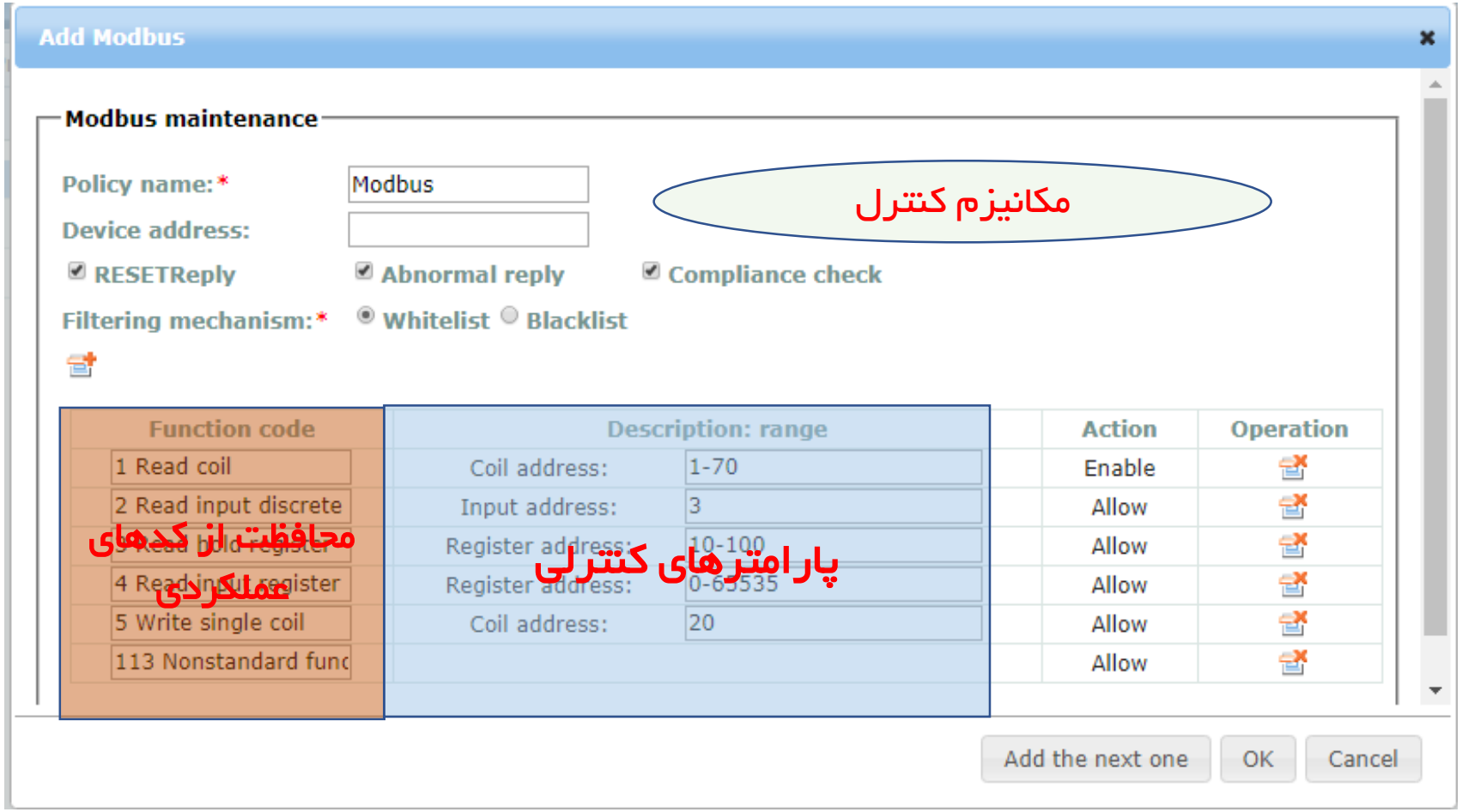
۴- قوانین امنیتی – پروتکل Modbus

- Modbus یک پروتکل ساده ارتباطی بین مبدل (Converter) و تجهیزات صنعتی است که در مقابل حملات بسیار آسیب پذیر می باشد. در واقع PLC با TCP:502 دستورات Modbus را برای مبدل می فرستد و مبدل با Modbus فرامین را به تجهیزات صنعتی ارسال می نماید.

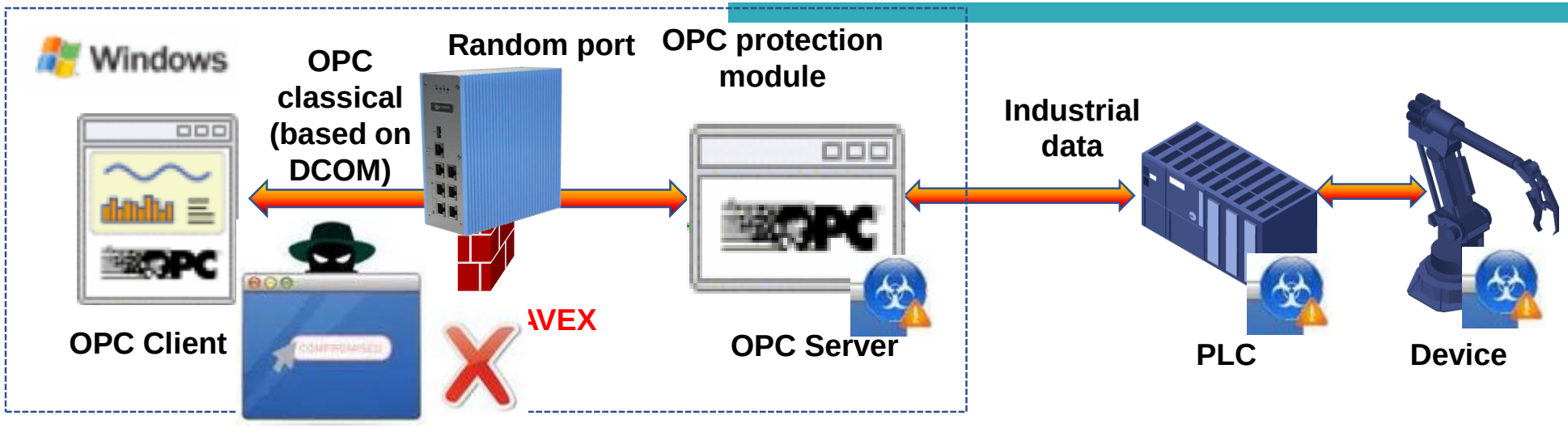
- محافظت کامل از پروتکل Modus
  - پارس کردن و محافظت از کدهای عملکردی
  - محافظت از آدرس های ثبات
  - کنترل متغیرهای گسسته
  - کنترل آدرس های ورودی
  - کنترل دامنه سیم پیچ
  - پاسخ به رخدادهای غیر نرمال
  - کنترل صحت و مطابقت با استاندارد
  - دارای امکان استفاده از لیست سیاه و لیست سفید

۴- قوانین امنیتی – پروتکل Modbus

تنظیمات



۴- قوانین امنیتی – پروتکل OPC



تهدید

OPC پروتکل انتقال داده است که بیشتر در صنایع زیرساختی، انرژی و تولیدی بکار برده می شود. این پروتکل بر اساس Microsoft DCOM دارای آسیب پذیری های امنیتی جدی می باشد. بدافزار HAVEX بر اساس OPC منتشر شده است.

پورت دینامیک

با استفاده از تکنولوژی پورت دینامیک DCOM، پروتکل کلاسیک OPC بطور تصادفی پورت های مختلفی را برای انتقال داده اختصاص می دهد. لذا توسط فایروال های سنتی نمی توان از آن محافظت کرد

محافظت از امنیت

ماژول Venusense OPC از تکنولوژی ردیابی پورت دینامیک استفاده می کند تا پورت های دینامیک را تشخیص دهد، سلامتی را کنترل کند و از پاکت های غیر نرمال جلوگیری کند.

۴- قوانین امنیتی – پروتکل OPC

- پروتکل OPC (OLE for Process Control) جهت انتقال اطلاعات از PLC به ERP بکار برده می شود. ERP ها دارای پایگاه داده بوده و امکان ذخیره سازی اطلاعات و ارائه داشبورد و گزارش دارند. پورت مورد استفاده این پروتکل بعد از برقراری ارتباط عوض می شود ولی حداکثر از ۴ تا پورت استفاده می کند.
- محافظت از پروتکل صنعتی OPC
  - بدون نیاز به تغییر تنظیمات OPC Sever و OPC Client
  - باز کردن رابط های دینامیک داده با استفاده از تکنولوژی ردیابی ارتباطات برای رابط های دینامیک (نیازی به باز کردن چند رابط نیست)
  - محافظت از OPC DA، HDA و پروتکل های A&E
  - بررسی درستی برای جلوگیری از پاکت هایی که با DCE/RPC مطابقت ندارند
  - محافظت از پایگاه داده و پایش امنیت داده های برنامه
  - محافظت از سیستم سنجش ایمنی

۴- قوانین امنیتی – پروتکل S7

- پروتکل S7 در PLC های سری S7 زیمنس (S7-200, 300, and 400) برای دانلود برنامه، کنترل و راه اندازی بکار برده می شود.
  - پارس کردن و محافظت از کدهای عملکردی
  - محافظت از آدرس های ثبات
  - کنترل متغیرهای گسسته
  - کنترل آدرس های ورودی
  - کنترل دامنه سیم پیچ
  - پاسخ به رخدادهای غیر نرمال
  - کنترل سلامت و مطابقت با استاندارد
  - دارای امکان لیست سیاه و لیست سفید

۴- قوانین امنیتی – پروتکل S7

تنظیمات

S7 maintenance

Policy name:* S7_test

☑ RESET reply ☑ Integrity check

کنترل در سطح فرامین

◉ Preset options

☑ Read only ☑ Read/Write ☑ Download ☑ Control ☑ Stop

○ Custom options

◉ Custom options

Filtering mechanism:* ◉ Whitelist ○ Blacklist

لیست سیاه و لیست سفید

Function code	Function block	Serial number	Address	Action	Operation
1 programmi	Action: 1 Data request 1			Enable	
29 upload	Block type: 56 OB	Serial number: 1		Allow	
40 Program c	Function: 1 insert			Allow	
7 Time	Action: 3 read 2			Allow	
41 PLC parkir				Allow	
				Allow	

محافظت از کدهای عملکردی

کنترل پارامترها

۴- قوانین امنیتی – پروتکل های شخصی سازی شده

- موتور سفارشی بسته ها را تجزیه و مدیریت می کند و به مشکل حفاظت در شرایطی که بسیاری از پروتکل های صنعتی خصوصی استفاده می شود پایان می دهد.
  - امکان خودتوسعه دادن، قابل کنترل و توسعه در محل
  - حفاظت از پروتکل های صنعتی خصوصی و متنوع که یکپارچه کردن آنها دشوار است
  - بیش از ۳۰۰ متغیر در پروتکل
  - بیش از ۵۰ عملکرد
  - بیش از ۲۰ کاراکتر عملیاتی
  - بیش از ۱۰ نوع داده
  - شخصی سازی قوانین در لایه های ۲ تا ۷

۴– قوانین امنیتی – پروتکل های شخصی سازی شده

Filtering mechanism

Filtering mechanism : ◉ Whitelist ○ Blacklist OK

Blacklist and whitelist

Custom rule list

	Sequence number	Rule number	Rule name	State	Operation
	1	10000001	ProfiNet-TCP/IP	⊗	Edit Enable
	2	10000002	ProfiNet-RT/IRT	⊗	Edit Enable

Add custom rules ✖

Rule configuration

Custom rule maintenance

Rule name:* s7_readvar

Protocol:* TCP

Detection feature:*

```
(tcp.dstport==102)&& (tcp.payload[0,0]=="\x03")&&
(tcp.payload[4,4]=="\x02")&&(tcp.payload[5,5]=="\xf0")&&
(tcp.payload[7,7]=="\x32")&&(tcp.payload[8,8]=="\x01")&&
oad[17,17]=="\x04")
```

Packet characteristics

Response mode:*

```
nothing()
```

Result ✖

Rule grammar check passed!

Check result

Grammar check

rammar check OK Reset Cancel

۴– قوانین امنیتی – پروتکل های شخصی سازی شده

Configuration manuals for online help

目 录
1 XDS概述
2 XDS支持的协议类型
2.1 XDS支持哪些协议
2.2 协议变量的分类
2.2.1 按存储类型分类
2.2.2 按报文方向分类
2.2.3 按报文类型分类
2.2.4 按载荷类型分类
2.3 协议变量的含义说明
2.3.1 ETHER协议
2.3.2 IP协议
2.3.3 ICMP协议
2.3.4 TCP协议
2.3.5 UDP协议
2.3.6 HTTP协议
2.3.7 DNS协议
2.3.8 FTP协议
2.3.9 SMTP协议
2.3.10 POP3协议
2.3.11 BGP协议
2.3.12 VLAN协议
2.3.13 MPLS协议
2.3.14 SIP协议
2.3.15 SCTP协议
2.3.16 IPSEC.AH协议
2.3.17 IPSEC.ESP协议
2.3.18 PPTP协议
2.3.19 L2TP协议
2.3.20 TELNET协议
2.3.21 IGMP协议
2.3.22 IEC104协议
2.3.23 MODBUS协议
3 XDS规则描述语言
3.1 主要特性
3.2 提及的概念
3.3 表达式是什么
3.4 XDS支持多少条规则
3.5 DOS还是UNIX格式
3.6 规则文件中使用汉字
3.7 规则中加入对K，M的支持
4 XDS的数据类型
4.1 整数(UINT)
4.1.1 表示整数常量
4.1.2 整数类型的细化
4.2 IP地址(IP)
4.3 IP地址数组(IPARRAY)
4.4 MAC地址(MACSTR)
4.5 字符串(BINSTR)
4.5.1 表示字符串常量
4.5.2 字符串中的转义符
4.6 时间(TIME)
4.7 集合变量(CVH)
4.8 布尔(BOOL)
4.9 VOID
4.10 浮点型(FLOAT)
5 XDS的运算符
5.1 运算符列表
5.2 运算符优先级
5.3 Grammar Disable错误
5.4 等于(eq)
5.5 不等于(ne)
5.6 大于(gt)
5.7 不小于(ge)
5.8 小于(lt)
5.9 不大于(le)
5.10 分号(;)

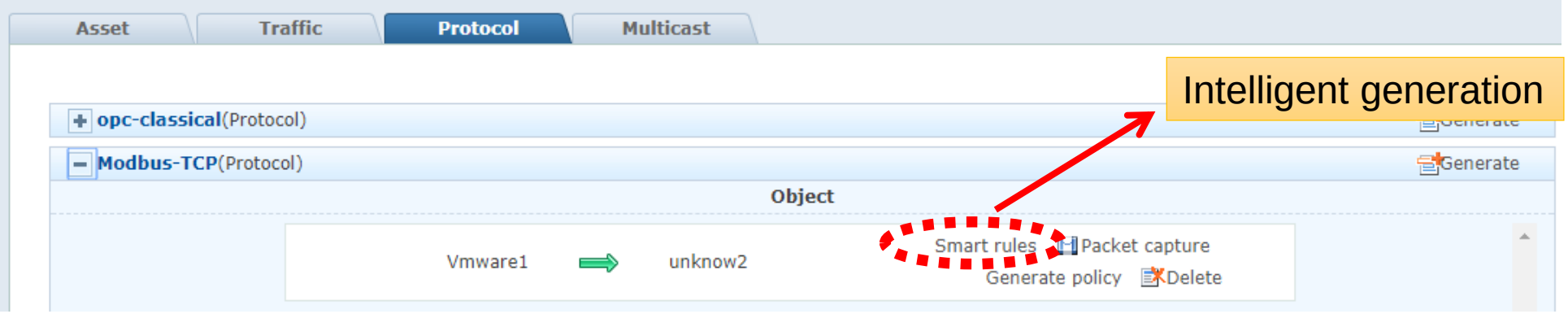
协议变量	数据类型	详细说明
ip.src	IP	源IP地址，192.168.0.1
ip.dst	IP	目的IP地址，192.168.0.1
ip.proto	UINT8	IP上层的协议
ip.version	UINT8	IP版本
ip.len	UINT16	IP报文长度
ip.hdr	POINTER	IP报文头
ip.hdr_len	UINT8	IP头长度
ip.payload	BINSTR	IP报文数据部分
ip.payload.len	UINT16	IP报文数据部分长度
ip.ident	INT	标示ID(13位片偏移)
ip.flags	INT	IP标志
ip.distance	INT	IP偏移
ip.xttl	INT	生存时间
ip.flag.rb	INT	保留位
ip.flag.df	INT	不可分片
ip.flag.mf	INT	分片位
ip.flag.num	INT	IP.FLAG.RB， IP.FLAG.DF，IP.FLAG.MF中置为1的个数
ip.service	INT	IP服务类型
ip.op.code	INT	IP选项类型（安全和处理限制：0X82、记录路径：0X07、时间戳：0X44、宽松源站选路）
ip.diffrence	INT	源和目的IP的差
ip.options	INT	IP选项
ip.options.len	INT	IP选项长度

۴- قوانین امنیتی – قوانین هوشمند

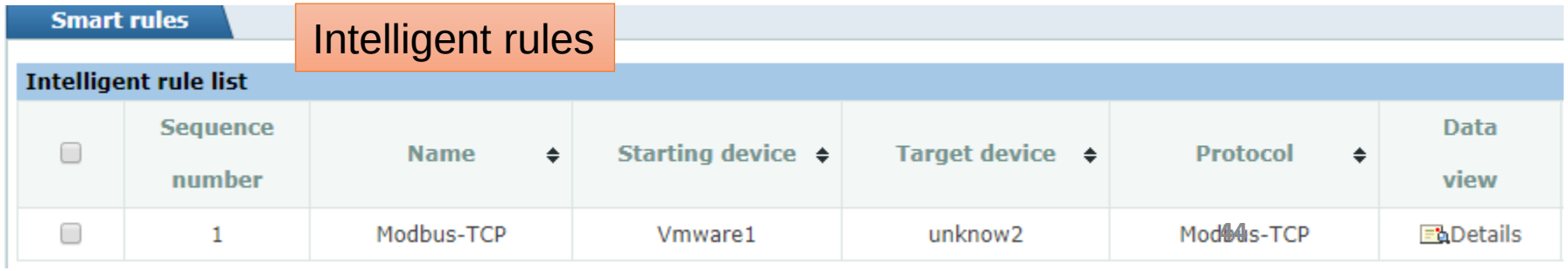
- قوانین هوشمند
  - کشف هوشمند پروتکل های صنعتی در حال اجرا
  - تشخیص محتوای پروتکل
  - ایجاد قوانین بر اساس مجموعه دستورات
  - پشتیبانی از Modbus و S7

Intelligent discovery

Intelligent generation



Intelligent rules



۴- قوانین امنیتی – سیستم پیش گیری از نفوذ

- شناسایی اقدامات نفوذی که براساس پروتکل های صنعتی یا آسیب پذیری ها انجام می شود، برای انجام حفاظت دینامیک
  - Protocol identification, abnormality inspection
  - Characteristics matching, dynamic protection

Modbus
IEC104
BACnet
DNP3
EthernetIP
Vulnerability
Modicon
NiagaraFox
SiemensS7

List of intrusion rules

	Sequence number	Rule number	Rule name	State	Operation
			Vulnerability		Enable
	1	28000001	TCP_CitectSCADA_ODBC overflow attacks		View Enable
	2	28000002	TCP_WonderWare-SuiteLink_ denial of service attack		View Enable
	3	28000003	TCP_RealWin-INFOTAG/SET_CONTROL packet processing, buffer overflow, attack events		View Enable
	4	28000004	TCP_ClearSCADA heap overflow attack events		View Enable
	5	28000005	TCP_Wonderware-InBatch_ buffer overflow attack events		View Enable
	6	28000006	TCP_Sielco-Sistemi-WinLog_ stack overflow attempt		View Enable
	7	28000007	TCP_RealWin-HMI-Service_ buffer overflow 1 event		View Enable
	8	28000008	TCP_RealWin-HMI-Service_ buffer overflow 2 event		View Enable
	9	28000009	TCP_RealWin-HMI-Service_ buffer overflow 3 event		View Enable

۴– قوانین امنیتی – Preset Scenario

- امکان استفاده از سیاست های از پیش تنظیم شده

Template details

List of template details

Siemens S7

	Sequence number	Rule number	Rule name	State	Operation
	1		S7	✓	Disable
	2	76000001	S7 links (phase one)	✓	Disable
	3	76000002	S7 links (stage two)	✓	Disable
	4	76000003	Read variable	✓	Disable
	5	76000004	Write variables	✓	Disable
	6	76000005	Program call service	✓	Disable
	7	76000006	PLC parking	✓	Disable
	8	76000007	Download	✓	Disable
	9	76000008	upload	✓	Disable
	10	76000009	Program function	✓	Disable
	11	76000010	Cyclic read data	✓	Disable
	12	76000011	CPU function	✓	Disable
	13	76000012	Block information	✓	Disable

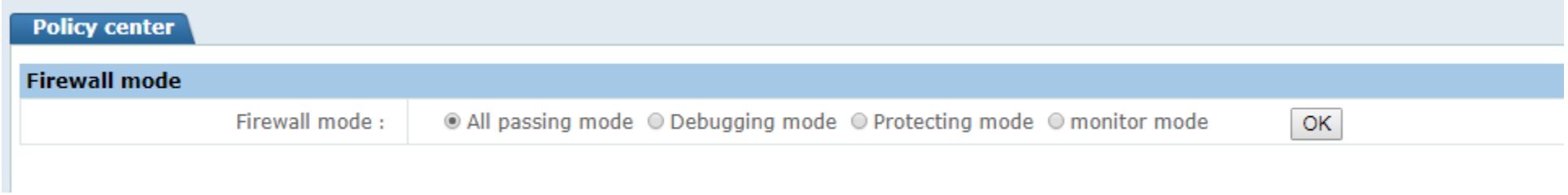
OK

۵. محافظت از شبکه – مرکز سیاست ها

حالات کاری

- **All passing mode**: No processing for traffic, physically going online.
- **Debugging mode**: Analyze and record logs for traffic, but not execute the action.
- **Protecting mode**: Strictly enforce the firewall policy.
- **Monitor mode**: Only analyze traffic.

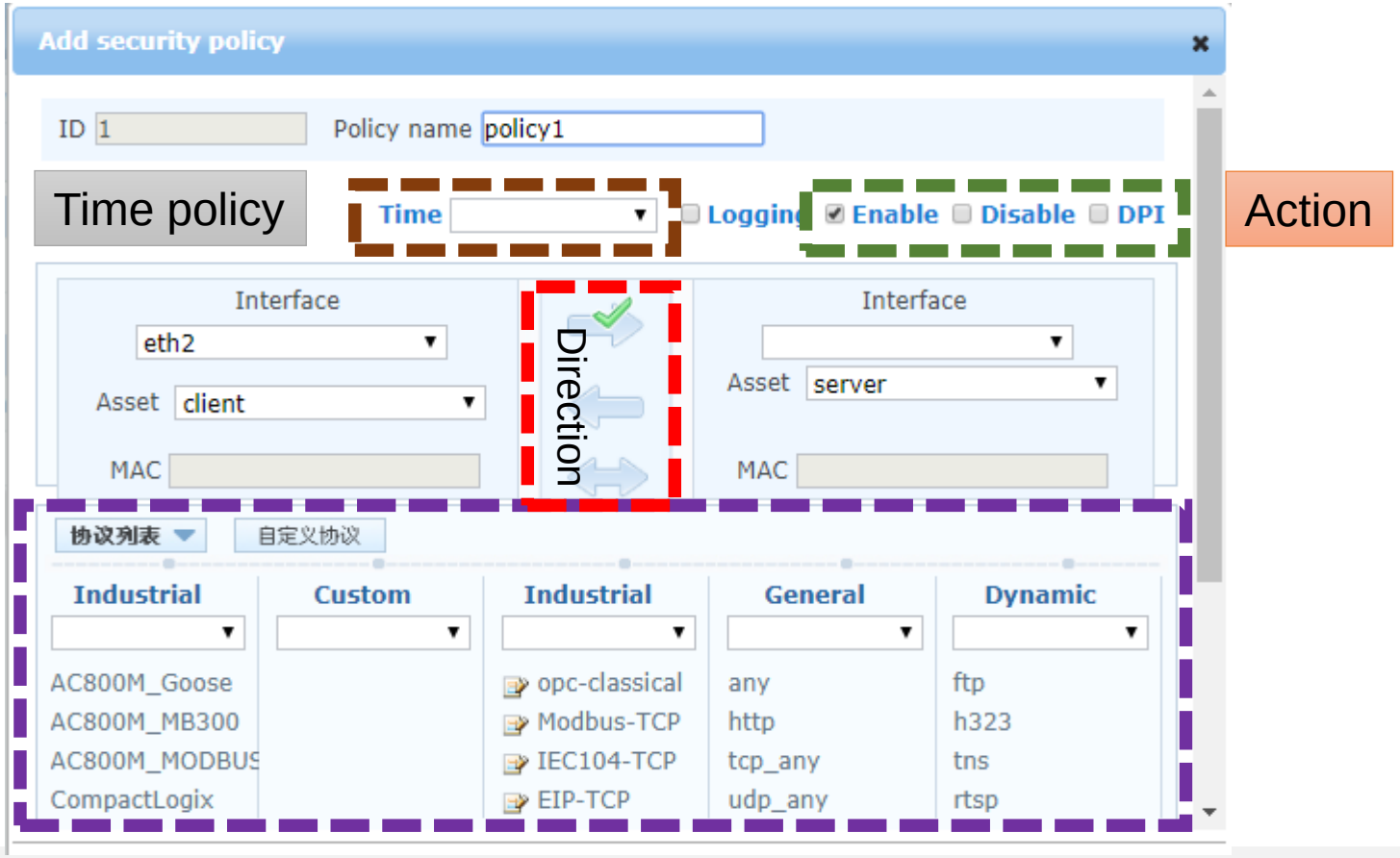
Configuration



۵. محافظت از شبکه – مرکز سیاست ها

سیاست های امنیتی

- Element: protocol, source asset, target asset, interface, action
- Direction: forward, backward, bidirectional
- Action: permit, deny, DPI (industrial protocols)



۵. محافظت از شبکه – Address Binding

- Admission control rules, IP and MAC address binding
  - Global admission control policy
  - Operation log recording and tracing
  - Uniqueness check

Address binding

Address-binding global settings: ☐ Enable IP/MAC check ☐ Record the binding log

OK

Enable IP/MAC address binding and configure the log

Bound IP/MAC pair

Binding list

	Sequence number	IP address	MAC address	Uniqueness check	Operation
☐	1	172.16.2.1	AA:0D:60:FD:00:C7	⊗	Edit Delete
☐	2	192.168.100.1	EE:0D:60:FD:00:C7	⊗	Edit Delete

New | Batch delete | Show 10 lines | Home | Previous | 1 | Next | Last | Jump to 1 page | GO

Create binding

Create a binding entry

Binding IP/MAC pair configuration

IPAddress:* 192.168.168.253

MACAddress:* ED:0D:60:FD:00:C9 (For example : 00:0D:60:FD:00:C7)

Uniqueness check: ☑

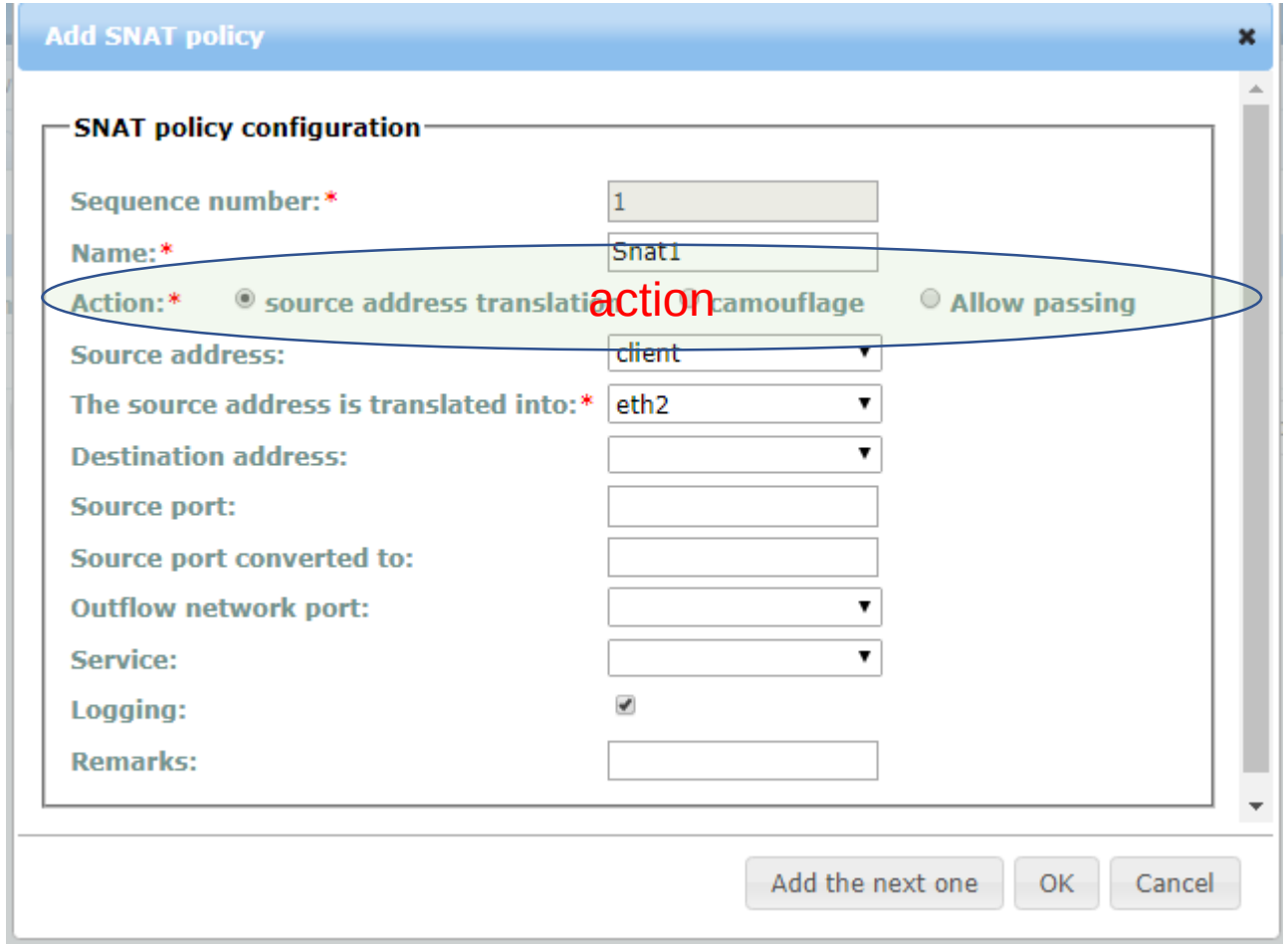
Enable uniqueness check

۵. محافظت از شبکه – NAT

- NAT type
  - SNAT (1-to-N, N-to-N)
  - Port mapping (N-to-N)
  - IP address mapping (1-to-1)
- Action
  - Forging: one-demand route NAT
  - Permit (exceptional, no NAT)

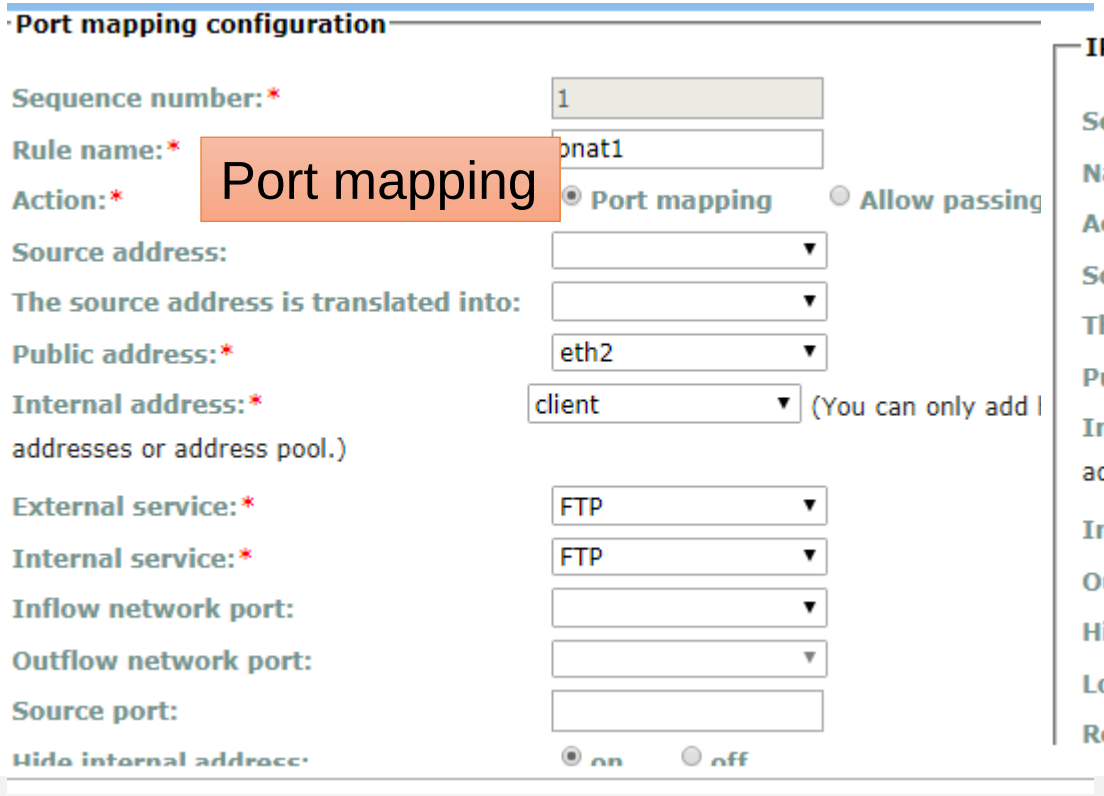
۵. محافظت از شبکه – NAT

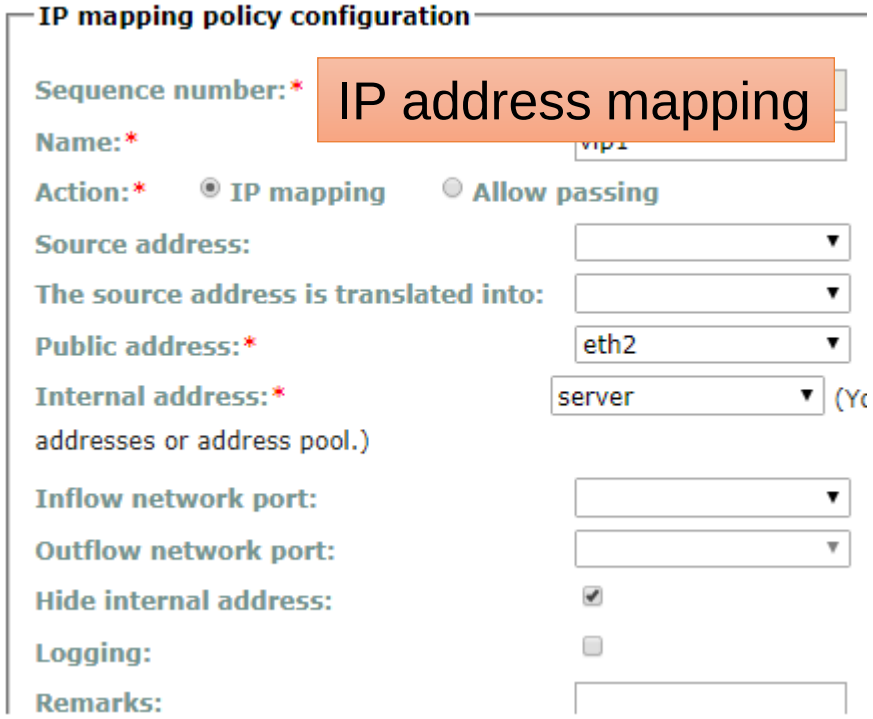
- SNAT
  - ✓ Source address: single address, network segment, address group, any
  - ✓ Post-translation address: single address, address pool, interface address



۵. محافظت از شبکه – NAT

- Port mapping/IP address mapping
  - ✓ Public address: interface IP address
  - ✓ Post-translation address: host address
  - ✓ Port/service: 1-to-1 port/service





۵. محافظت از شبکه – پروتکل ها

- مدل محافظت صنعتی

✓ Preset security protection models for industrial devices according to vendor.

COPA(Vendor)		Add Edit Delete Delete
Emerson(Vendor)		Add Edit Delete Delete
GE-Fanuc(Vendor)		Add Edit Delete Delete
General-Electric(Vendor)		Add Edit Delete Delete
HIMA(Vendor)		Add Edit Delete Delete
Honewell(Vendor)		Add Edit Delete Delete
MTL(Vendor)		Add Edit Delete Delete
Mitsubishi-Electric(Vendor)		Add Edit Delete Delete
OMRON(Vendor)		Add Edit Delete Delete
OPTO(Vendor)		Add Edit Delete Delete
Schneider(Vendor)		Add Edit Delete Delete
Siemens(Vendor)		Add Edit Delete Delete
Product model	**Protocol list**	**Remarks**
SIMATIC-S7200	dhcp_udp_client; http; FTE_Multicast; IEC_MMS; PROFINET_Context_Manager_UDP; PROFINET_Multicast_TCP; PROFINET_Multicast_UDP; PROFINET_Unicast_TCP; PROFINET_Unicast_UDP	
SIMATIC-S7300		
SIMATIC-S7400		
SIMATIC-S7400FH		
SIMATIC-S7-C		
S7-Series		
Wago(Vendor)		Add Edit Delete Delete
Yokogawa(Vendor)		Add Edit Delete Delete

۵. محافظت از شبکه – پروتکل ها

- Preset the industrial protocol.
  - The mainstream industrial protocols are preset in the system.

Preset industrial protocol

Sequence number	Name	Protocol
1	ABB_CNCP	IP protocol, port:3341(UDP)
2	Cisco_Conf	Non-IP protocol number:0x9000
3	COPA_Driver_Simulation	IP protocol, port:6000(TCP)、6020(TCP)
4	COPA_Straton_Event_Port	IP protocol, port:911(TCP)
5	COPA_Stratonrt	IP protocol, port:1200-1210(TCP)、4500-4510(TCP)、7000-7010(TCP)、9000-9010(TCP)
6	GOOSE_IEC61850	Non-IP protocol number:0x88B8
7	Intel_NTC	Non-IP protocol number:0x886d
8	LLDP	Non-IP protocol number:0x88cc
9	MRP_IEC62439	Non-IP protocol number:0x88E3
10	Reverse_ARP	Non-IP protocol number:0x8035

Show 10 lines | Home | Previous | 1 | 2 | 3 | ... 9 | Next | Last | Jump to 1 page | GO

- Customize protocols.
  - Customize protocols and ports according to service requirements.

Custom protocol

	Sequence number	Service name	Protocol	Operation
	1	customP	TCP (8080,8080)-(0,65535)	Edit Delete

Add | Batch delete

Show 10 lines | Home | Previous | 1 | Next | Last | Jump to 1 page | GO

۵. محافظت از شبکه – پروتکل ها

- Universal protocols: involve all mainstream network protocols.

Preset general protocol

Sequence number	Name	Protocol	Port	Protocol overview
1	AH	51	All	Authentication Header protocol
2	AUTH	TCP	113	
3	BGP	TCP	179	
4	Bootstrap_Cli	UDP	68	Bootstrap_Client service
5	Bootstrap_Serv	UDP	67	Bootstrap_Server(DHCP) service
6	Chargen_tcp	TCP	19	Chargen_tcp service
7	Chargen_udp	UDP	19	Chargen_udp service
8	EFS	TCP	520	EFS
9	EGP	EGP	All	Exterior Gateway Protocol
10	ESP	50	All	Encapsulation Security Payload protocol

Universal protocols

1 page GO

Dynamic protocol

	Sequence number	Protocol name	Protocol	Remarks	Operation
	1	ftp	FTP(21)	default service...	Edit
	2	h323	H.323(1720)		Edit
	3	h323_gk	H323_GK(1719)		Edit
	4	irc	IRC(6667)	default service...	Edit
	5	mms	MMS(1755)	default service...	Edit
	6	rtsp	RTSP(554)	default service...	Edit
	7	sip	SIP(5060)	default service...	Edit
	8	tftp	TFTP(69)	default service...	Edit
	9	tns	TNS(1521)	default service...	Edit
	10	xdmcp	XDMCP(177)	default service...	Edit

Dynamic protocols

۵. محافظت از شبکه – دارایی ها (Assets)

- Assets
  - Host address
  - Network address
  - Exclusive IP address
  - Address range
- Asset group
  - A set of multiple assets
- Asset pool
  - A set of multiple host addresses
  - 1-254 addresses supported
- A total of 1024 addresses are supported.

۵. محافظت از شبکه – دارایی ها (Assets)

Asset

Asset list maintenance

Name:* dnc-server1

Asset definition method: IP address/mask anti-IP address

Address range

IPv4 address:* 192.168.168.253 / 255.255.255.255

Remarks:

Definition method

Asset group

Asset group maintenance

Name:* group1

Add element table to asset group

Asset list member

client
server
cc

>>

<<

Asset group member

S1
s3

Asset list

Member list

Remarks:

Add asset pool

Asset pool

Asset pool configuration

Name:* a_pool

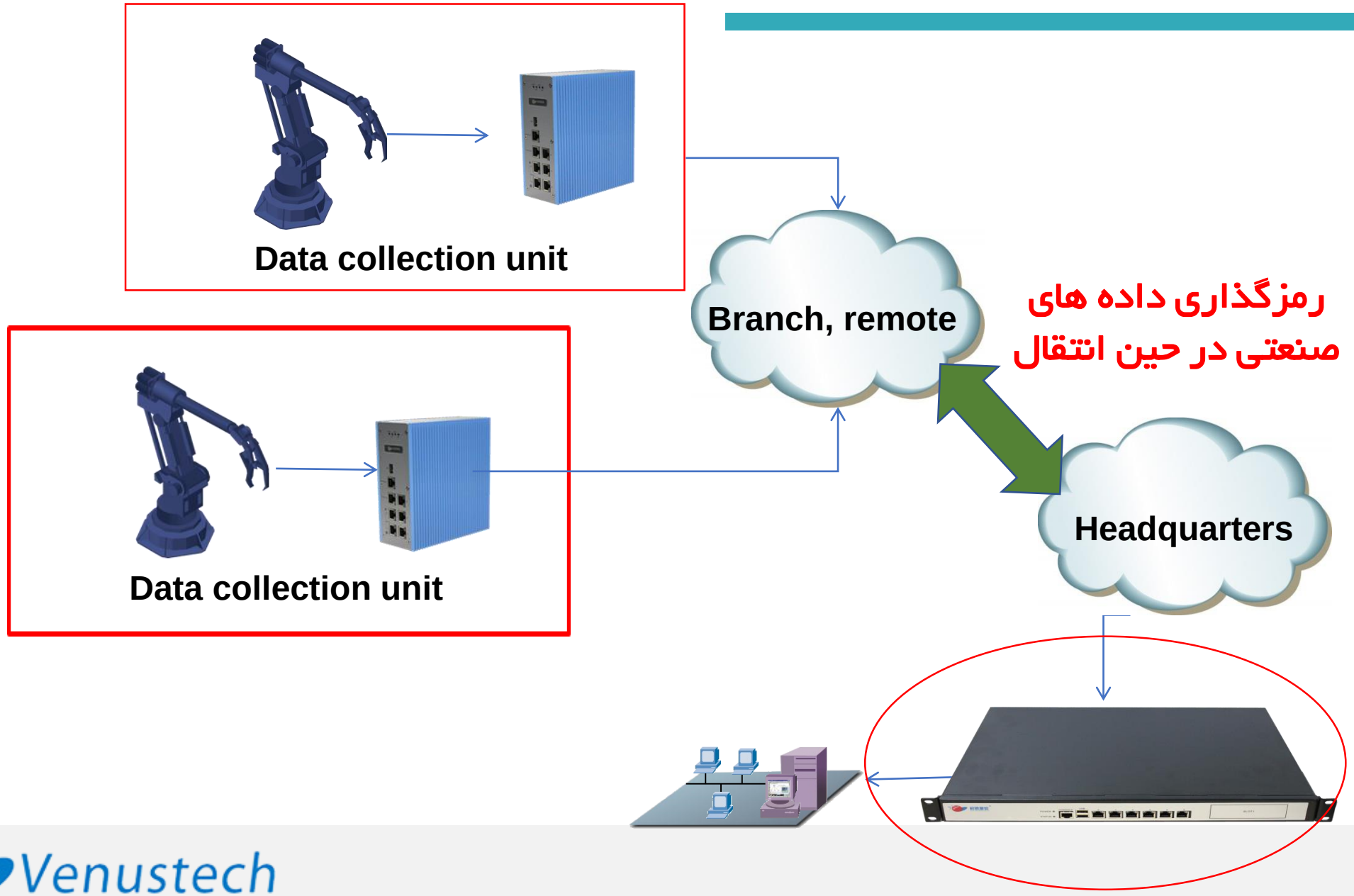
Asset:* 192.168.1.1 - 2.2.2.2

Remarks:

IP address segment can contain up to 254 IP addresses.

An asset pool has up to 254 addresses.

۶. VPN صنعتی


Data collection unit
Data collection unit
Branch, remote
رمزگذاری داده های
صنعتی در حین انتقال
Headquarters

۶. VPN صنعتی

مجموعه پروتکل ها

Add IKE configuration

IKE configuration

Name:*	IKE
Type:*	Gateway
Peer address type:*	IP address
Peer address:*	172.16.2.1
Protocol type:	International standard
Authentication method:	Pre-shared key
Pre-shared key:*	TypeYourPrekey

Advanced options

VPN protocol set:

1-Encryption algorithm	aes128	Authentication	sha1
algorithm	aes128	Authentication	md5
algorithm	3des	Authentication	sha1
4-Encryption algorithm	3des	Authentication	md5

IKE protocol set

DH group: 1 2 5

Key period: 28800

Negotiation mode: Aggressive mode Main mode

Whether to set ID:

Mode configuration

Add VPN tunnel configuration

VPN tunnel configuration

Tunnel name:*	test
Local outlet:*	
Binding IKE:*	
Associate VPN rules:*	
Whether to enable:	

Advanced options

VPN protocol set:

1 - Encryption algorithm	aes128	Authentication	sha1
2 - Encryption algorithm	aes128	Authentication	md5
3 - Encryption algorithm	3des	Authentication	sha1
4 - Encryption algorithm	3des	Authentication	md5

VPN protocol set

VPN protocol:* ESP AH

Key period (seconds): 3600

Transport mode: Tunnel mode Transport mode

Perfect forward secrecy:

۷. امنیت رابط سریال – Serial DPI (Deep Packet Inspection)

- Serial link
  - RS232/485
- Modbus protocol protection based on serial link
  - Protect function code parsing.
  - Protect register addresses.
  - Control discrete variables.
  - Control input addresses.
  - Control the coil range.
  - Respond to abnormalities.
  - Check integrity and standard compliance.
  - Support blacklist and whitelist.

۷. امنیت رابط سریال – Serial DPI (Deep Packet Inspection)

Interface settings list

Device name	Operating mode	Baud rate	Data bit	Parity check	Stop bit	Traffic control	Operation
ttyS0	Management	9600	8	No parity	1	No traffic control	
	Communication	9600	8	No parity	1	No traffic control	OK
ttyS1	Management	9600	8	No parity	1	No traffic control	
	Communication	9600	8	No parity	1	No traffic control	OK

Switch operating modes

Switch serial port working mode

Associate interfaces with policies

Policy configuration

Master interface :	ttyS0	DPI :	Modbus	Logging :		OK

Modbus maintenance

Policy name:* Modbus

Device address:

RESETReply Control mechanism Protocol compliance check

Filtering mechanism:* Whitelist Blacklist

Policy configuration

Function code	Description: range		Action	Operation
1 Read coil	Coil address:	1-70	Enable	
2 Read discrete	Input address:	3	Allow	
3 Read hold register	Register address:	10-100	Allow	
4 Read input register	Register address:	0-65535	Allow	
5 Write single coil	Coil address:	20	Allow	
113 Nonstandard func			Allow	

Protect function codes

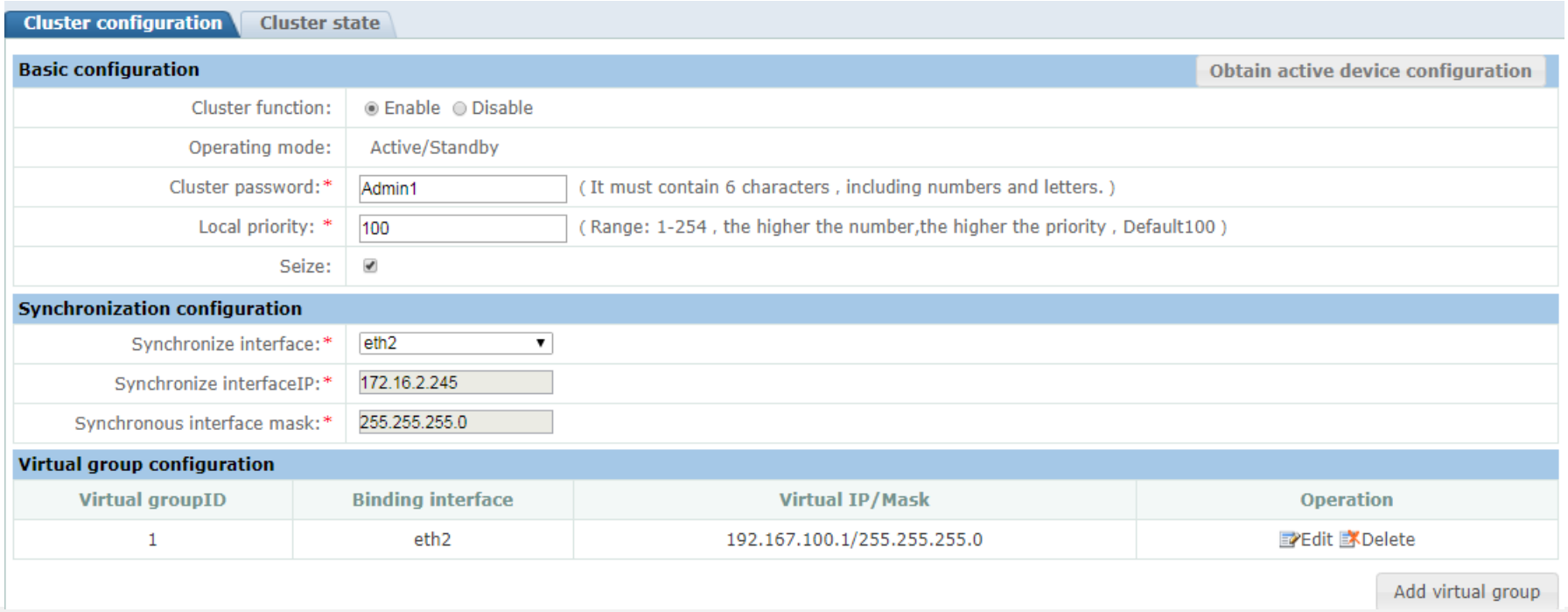
Control parameters

۸. High Availability (HA)

- Hardware bypass
  - Software failure bypass
  - Hardware failure bypass
  - Power-off bypass
- HA
  - Real-time status monitoring, real-time response
  - Automatic synchronization of core configurations to the backup system
  - Seamless switchover, service guarantee anytime

High Availability (HA) .۸

- HA configuration
  - Master/backup mode
  - Master/slave identities verification
  - Interfaces and interface IP addresses for master/slave status synchronization
  - Service interfaces and IP addresses (virtual group)



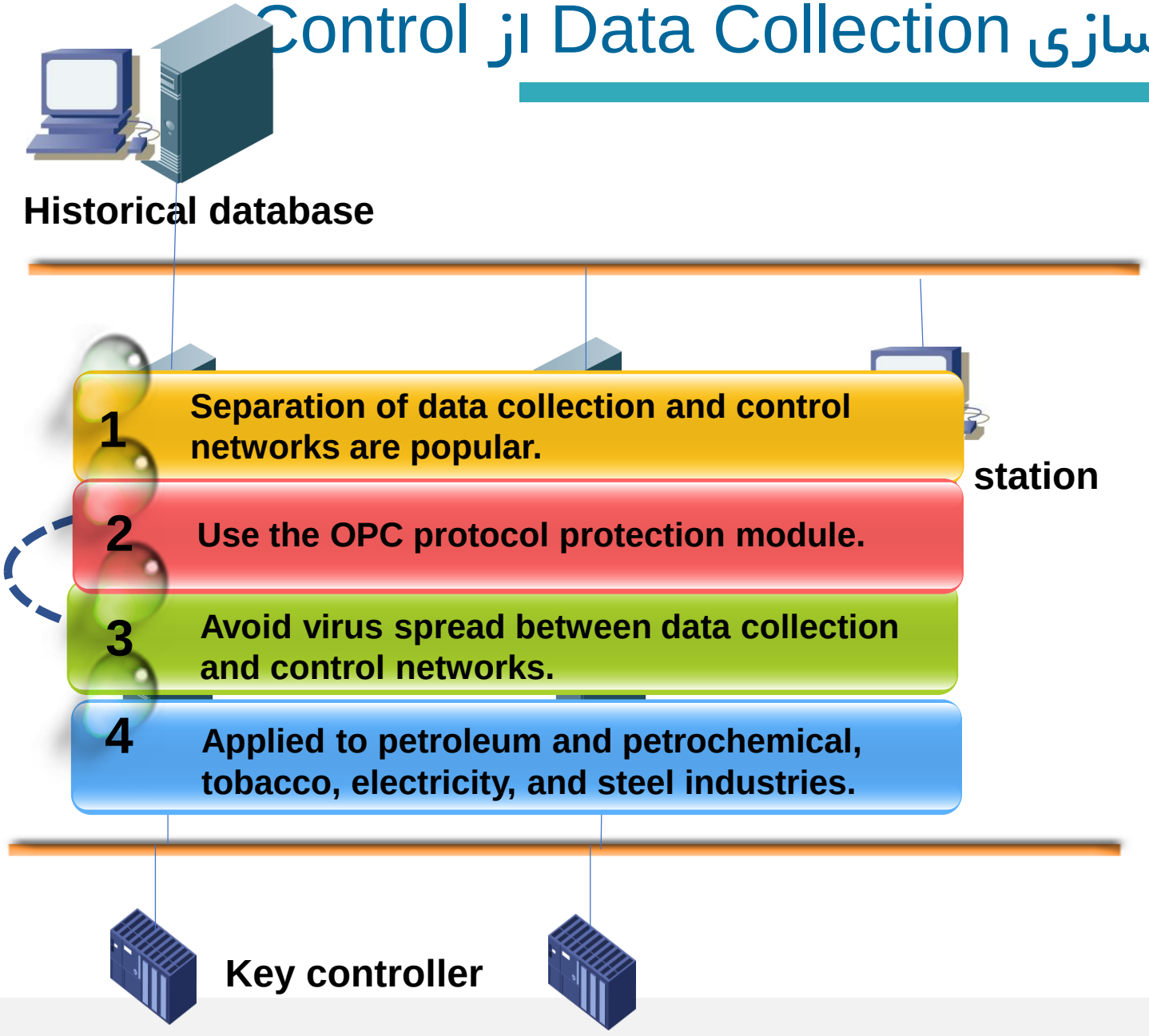
Log .۹

- Log
  - Report: reporting based on event level
  - Storage: local and server storage
  - Interface: standard syslog interface
  - Export: local PC, USB flash drive
  - Check: checking in web and file modes
  - Overflow mechanism: overwrite, stop
  - Log content
    - ✓ Time, type, level, details
    - ✓ Service source IP address, destination IP address, protocol, module
    - ✓ Detailed logs recorded at the function code level

کاربردهای معمول

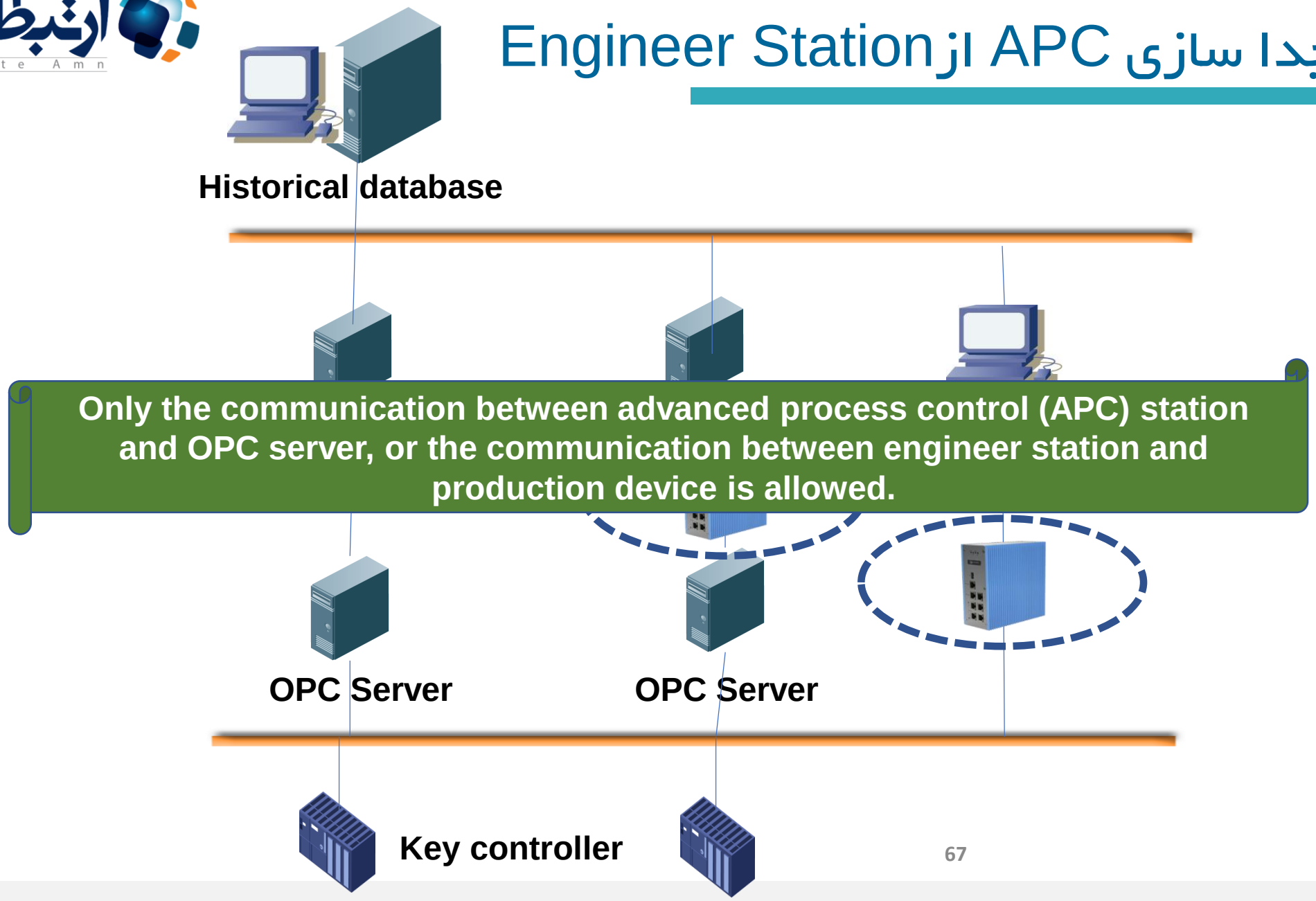
کاربردهای
معمول

کاربرد اول: جدا سازی Data Collection از Control

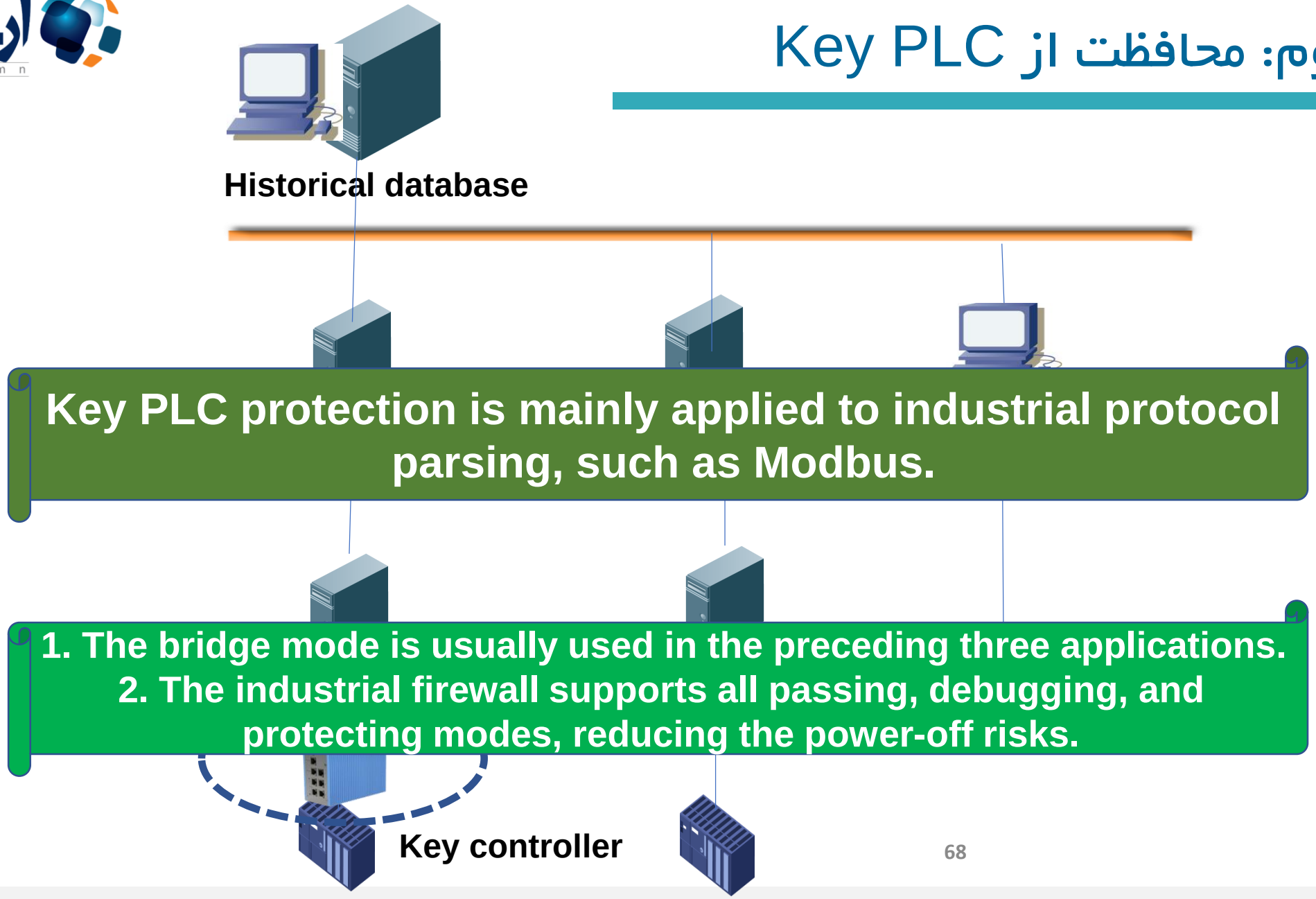


1. Separation of data collection and control networks are popular.
2. Use the OPC protocol protection module.
3. Avoid virus spread between data collection and control networks.
4. Applied to petroleum and petrochemical, tobacco, electricity, and steel industries.

کاربرد دوم: جدا سازی APC از Engineer Station



کاربرد سوم: محافظت از Key PLC



ارتباط امن

Ertebate Amn

Thank you